(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－305662

(43)公開日　平成８年(1996)11月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０Ｃ
	13/00	３５１	7368－5E		13/00	３５１Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 22 頁）

(21)出願番号　特願平7－108408

(22)出願日　平成７年(1995)５月２日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　宗像　昭夫
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　遠山　勉　（外１名）

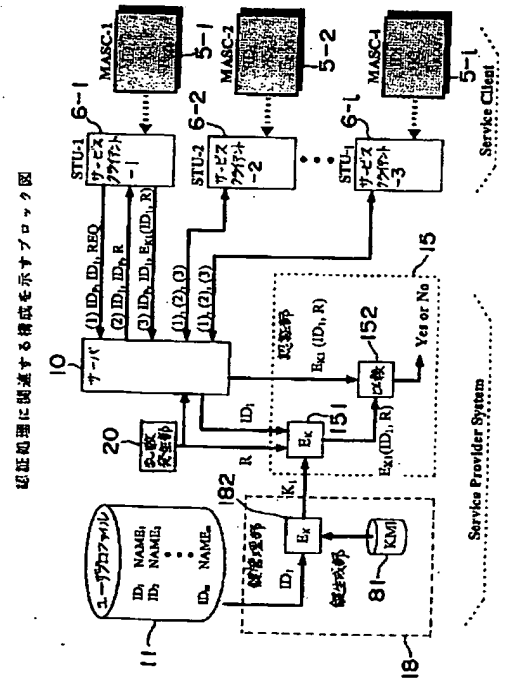
最終頁に続く

(54)【発明の名称】　クライアント認証システムおよび方法

(57)【要約】

【目的】クライアントとサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方おいて動的に作成することにより、これらの第三者による盗用が不可能となるクライアント認証システムを提供する。

【構成】サービス提供者側システム１の鍵管理部１８は、アクセス要求を行ったサービスクライアント６に接続されたＭＡＳＣ５に対応する個別鍵Ｋを生成し、この個別鍵Ｋを認証部１５に通知する。この個別鍵は、予め、ＭＡＳＣ５にも格納されている。乱数発生器２０は、乱数Ｒを生成して、ＭＡＳＣ５に送信するとともに、認証部１５に通知する。ＭＡＳＣ５は、この乱数を個別鍵によって暗号化して、サービス提供者側システム１に戻す。一方、認証部１５の暗号化部１５１は、乱数Ｒを個別鍵Ｋによって暗号化する。そして、認証部１５の比較器１５２は、暗号化部１５１が暗号化したデータとＭＡＳＣから送信されてきた暗号化データを比較して、両者が一致した場合には、このＭＡＳＣ５からのアクセス要求であると確認する。



【特許請求の範囲】
【請求項1】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、
前記データ供給装置は、
前記クライアントに対応する第1の鍵を出力する鍵出力部と、
前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、
前記鍵出力部において出力されたされた第1の鍵によって前記乱数を暗号化することによって第1の認証子を出力する第1の暗号化手段と、
前記クライアントに前記乱数を送信する第1の送信手段と、
前記クライアントから第2の認証子を受信する第1の受信手段と、
前記第1の認証子と前記第2の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、
前記クライアントは、
前記データ供給装置にアクセス要求を行うアクセス要求手段と、
前記データ供給装置から送信された前記乱数を受信する第2の受信手段と、
前記第1の鍵と同一の第2の鍵を保持する鍵保持手段と、
前記第2の鍵によって前記乱数を暗号化することによって前記第2の認証子を出力する第2の暗号化手段と、
前記データ供給装置に前記第2の認証子を送信する第2の送信手段とを備えることを特徴とするクライアント認証システム。
【請求項2】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、
前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第1の鍵を生成することを特徴とする請求項1記載のクライアント認証システム。
【請求項3】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送することを特徴とする請求項1記載のクライアント認証システム。
【請求項4】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、
前記クライアントは前記暗号化された前記データを複合化する第1の復号化手段を備えることを特徴とする請求項1記載のクライアント認証システム。
【請求項5】前記データ供給装置は前記データを復号化するための第3の鍵を前記第1の鍵によって暗号化する第3の暗号化手段を備えているとともに、
前記クライアントは前記暗号化された前記第3の鍵を前記第2の鍵によって復号化する第2の複合化手段を備え、
前記第1の復号化手段はこの第2の複合化手段によって復号化された前記第3の鍵によって前記暗号化されたデータを復元することを特徴とする請求項4記載のクライアント認証システム。
【請求項6】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、
一方の格納装置に格納されている前記暗号化されたデータを前記第3の鍵を用いて復号化する第3の復号化手段と、
第3の鍵を更新する鍵更新手段と、
第3の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第3の鍵によって暗号化する第3の暗号化手段と、
第3の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えたことを特徴とする請求項5記載のクライアント認証システム。
【請求項7】前記第3の復号化手段，前記鍵更新手段，前記第3の暗号化手段，及び前記書込手段は一定時間毎に起動することを特徴とする請求項6記載のクライアント認証システム。
【請求項8】前記クライアントは、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成されるとともに、
少なくとも前記鍵保持手段及び前記第2の暗号化手段は前記モジュール部に備えられていることを特徴とする請求項1記載のクライアント認証システム。
【請求項9】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、
前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、
前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第1の鍵によって前記乱数を暗号化して第1の認証子に変換し、
前記クライアントは前記第1の鍵と同一内容を有するものとして予め保持している第2の鍵によって前記乱数を暗号化して第2の認証子に変換するとともに、この第2の認証子を前記データ供給装置に送出し、
前記データ供給装置は前記第1の認証子と前記第2の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とするクライアント認証方法。
【発明の詳細な説明】
【0001】

【産業上の利用分野】本発明は、クライアントからの要求に応じて、映像著作物等のソフトウエアを通信手段を介して配送するシステム（デジタル・オーディオ・インタラクティブ・システム）におけるクライアント認証システム及び認証方法に関する。

【０００２】

【従来の技術】近年、ケーブルテレビジョンシステムや通信衛星を用いた通信システムの構築を背景に、デジタル情報化されたソフトウェア（音声データ，映像データ等，以下、「コンテンツ」という）を各家庭等に配送するサービスが提案されている。このサービスシステムは、ビデオ・オン・デマンド方式等と呼ばれるデジタル・オーディオ・インタラクティブ・システムである。このデジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者とユーザとの間で電話線等を介した通信が行われる。そして、サービス提供者は、ユーザから要求された時刻に要求された内容のコンテンツをこのユーザに配送するとともに、このソフトウェアの使用料金をクレジットカード会社等を通じて当該ユーザに課金し、その一部をコンテンツ供給者に還元するのである。

【０００３】このようなデジタル・オーディオ・インタラクティブ・システムが普及してゆく上で重要な事は、インフラストラクチャーとなるサーバ/ ネットワーク/ ターミナルが低コストで構築されることは勿論であるが、これらを媒介としてユーザに提供されるコンテンツが豊富に準備されなければ、成功とはならないということである。即ち、コンテンツとインフラストラクチャは車の両輪であるので、コンテンツ提供者がコンテンツ提供による利益回収を見込めるとともに不測の損害を被る危険がない仕組みをこのインフラストラクチャに組み込むことにより、コンテンツが集まりやすい環境を整備することが不可欠なのである。なお、このような仕組みは、コンテンツ提供者とユーザとを媒介する供給メディアの種類（広帯域ケーブルネットワーク，衛星システム，移動通信，光メディアパッケージ等）に拘わらず、整備されていなければならない。

【０００４】このような環境の整備がなされることにより、コンテンツ供給者は、安心して気軽に、コンテンツを供給することができるようになる。一方、ユーザは、いつでもどこでも、簡単な手続きによって必要なコンテンツを入手できるようになる。このことが、システムをより一層普及させるために重要なポイントとなっているのである。

【０００５】一方、システム構築に当たっては、誰もが参加できるオープン性が重要であり、既存の標準技術を可能な限り活用する方式を取っていくことが必要である。また、技術の進歩や各種サービスの多様化に対応できる拡張性も持ち合わせたものであることを併せて考慮すべきである。

【０００６】

【発明が解決しようとする課題】以上説明したように、デジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者は、コンテンツ配送を要求してきたユーザが誰であるのかを正確に識別して、確実に課金することができなければならない。即ち、課金を行うために必要なデータ（例えば、クレジットカード番号，銀行口座番号，等）を登録していない第三者がこれらデータを登録しているユーザになりすましてコンテンツの配送を受けてしまうことを、防止しなければならない。そのため、登録されているＩＤコードとコンテンツ配送を行ったユーザのＩＤコードとを照合する認証システムが提案されている。

【０００７】しかしながら、このようなＩＤコードによる認証システムでは、ＩＤコードが第三者によって盗まれた場合においてこの第三者による盗用を防止する手だてはない。なお、ＩＤコードにパスワードを付する方式も提案されているが、盗まれた場合に第三者の盗用が可能であることには変わりがない。

【０００８】そこで、本発明の第１の課題は、ユーザ（クライアント）とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方おいて動的に作成することにより、第三者の盗用が不可能となるクライアント認証システムを提供することである。

【０００９】また、単純なＩＤコードによって認証を行うシステムであるならば、ユーザがこのＩＤコードをマニュアルで入力できるので、コンテンツの配送要求を行った個々人毎の認証も可能であるが、複雑な識別情報を扱う場合であると、識別情報の動的な作成は勿論、マニュアルによる識別情報の入力でさえも不可能となってしまう。従って、従来提案されていた認証システムでは、コンテンツの再生を行う再生装置が自動的に認証作業を実行し、この再生装置毎に認証を行うようになっていた。

【００１０】しかしながら、再生装置毎に認証を行うのであると、複数の再生装置を有している場合には、再生装置毎に課金のためのデータを登録しなければならない。また、自己の課金のためのデータがサービス提供者に登録されている場合であっても、例えば他人に借りた再生装置でコンテンツを再生することは一切できなくなってしまう。このように硬直したシステムであると、上述した理由によりシステム普及はおぼつかない。

【００１１】そこで、本発明の第２の課題は、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着できるモジュールに、認証を行うためのデータ及び機能を持たせたクライアント認証システムを提供することである。

【００１２】

【課題を解決するための手段】

（第１の課題を解決するための手段）本発明によるクライアント認証システムの第１の態様は、上記第１の課題を解決するために、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、前記データ供給装置は、前記クライアントに対応する第１の鍵を出力する鍵出力部と、前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、前記鍵出力部において出力されたされた第１の鍵によって前記乱数を暗号化することによって第１の認証子を出力する第１の暗号化手段と、前記クライアントに前記乱数を送信する第１の送信手段と、前記クライアントから第２の認証子を受信する第１の受信手段と、前記第１の認証子と前記第２の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、前記クライアントは、前記データ供給装置にアクセス要求を行うアクセス要求手段と、前記データ供給装置から送信された前記乱数を受信する第２の受信手段と、前記第１の鍵と同一の第２の鍵を保持する鍵保持手段と、前記第２の鍵によって前記乱数を暗号化することによって前記第２の認証子を出力する第２の暗号化手段と、前記データ供給装置に前記第２の認証子を送信する第２の送信手段とを備えることを特徴とする（請求項１に対応）。

【００１３】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第１の鍵を生成するようにしても良い（請求項２に対応）。

【００１４】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送するようにしても良い（請求項３に対応）。

【００１５】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、前記クライアントは前記暗号化された前記データを複合化する第１の復号化手段を備えるようにしても良い（請求項４に対応）。

【００１６】前記データ供給装置は前記データを復号化するための第３の鍵を前記第１の鍵によって暗号化する第３の暗号化手段を備えているとともに、前記クライアントは前記暗号化された前記第３の鍵を前記第２の鍵によって復号化する第２の複合化手段を備え、前記第１の復号化手段はこの第２の複合化手段によって復号化された前記第３の鍵によって前記暗号化されたデータを復元するようにしても良い（請求項５に対応）。

【００１７】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、一方の格納装置に格納されている前記暗号化されたデータを前記第３の鍵を用いて復号化する第３の復号化手段と、第３の鍵を更新する鍵更新手段と、第３の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第３の鍵によって暗号化する第３の暗号化手段と、第３の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えるように構成しても良い（請求項６に対応）。このように格納装置を二重化する事によりデータのバックアップができるとともに、暗号化した鍵をその都度更新するので、データのセキュリティを向上させることができる。

【００１８】なお、前記第３の復号化手段，前記鍵更新手段，前記第３の暗号化手段，及び前記書込手段を一定時間毎に起動するようにしても良い（請求項７に対応）。本発明によるクライアント認証方法は、上記第１の課題を解決するため、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第１の鍵によって前記乱数を暗号化して第１の認証子に変換し、前記クライアントは前記第１の鍵と同一内容を有するものとして予め保持している第２の鍵によって前記乱数を暗号化して第２の認証子に変換するとともに、この第２の認証子を前記データ供給装置に送出し、前記データ供給装置は前記第１の認証子と前記第２の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とする（請求項９に対応）。

（第２の課題を解決するための手段）本発明の前記クライアント認証システムの第２の態様は、前記第１の態様におけるクライアントを、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成するとともに、少なくとも前記鍵保持手段及び前記第２の暗号化手段は前記モジュール部に備えるように構成したことを特徴とする（請求項８に対応）。なお、上述の識別情報を使用する場合には、この識別情報はこのモジュール部に格納しておく。また、上述の第１の複合化手段及び第２の複合化手段を設ける場合には、これら複合化手段をこのモジュール部に格納する。

【００１９】

【作用】本発明の第１の態様によると、クライアントのアクセス要求手段がデータ供給装置にアクセス要求を行うと、このアクセス要求に応じて、データ供給装置の乱数発生部が乱数を発生するとともに、鍵出力部がこのクライアントに対応する第１の鍵を出力する。そして、第

１の通信手段は、アクセス要求元のクライアントに乱数を送信する。また、第１の暗号化手段は、鍵出力部において出力された第１の鍵によって乱数を暗号化することにより、第１の認証子を出力する。一方、クライアントの第２の受信手段が乱数を受信すると、第２の暗号化手段は、鍵保持手段が保持している前記第１の鍵と同一の第２の鍵によってこの乱数を暗号化することにより、第２の認証子を出力する。この第２の認証子は、第２の送信手段によってデータ供給装置に送信される。データ供給装置の第１の受信手段がこの第２の認証子を受信すると、比較手段が第１の認証子と第２の認証子とを比較して、両者が一致している場合に当該クライアントからのアクセス要求であると認証する。従って、通信インタフェース上で送信される識別のための情報（認証子）は暗号化されたものであって、その暗号化された結果は乱数に従って変化するので一定にはならない。そのため、第三者による盗用が不可能になる。

【００２０】本発明の第２の態様によると、クライアントを構成する各構成部のうち、認証に必要なデータを保持する構成部（鍵保持手段）や認証に必要な処理を行うための構成部（第２の暗号化手段）のみを、本体部から着脱自在に設けたモジュール部に備えるようにしたので、誰の所有による本体部であっても、ユーザが自分のモジュール部を接続してデータの配送を受けることができる。

【００２１】

【実施例】以下、図面に基づいて、本発明の一実施例の説明を行う。本実施例は、本発明によるクライアント認証システムを、デジタル・オーディオ・インタラクティブ・システムに適用したものである。なお以下の説明においては、コンテンツを再生するためのコンテンツ再生装置のことを、「サービスクライアント」という。

《実施例の構成》

（システムの全体構成）本実施例によるデジタル・オーディオ・インタラクティブ・システムを図１に示す。このシステムは、多数のコンテンツを格納するとともにこのコンテンツを配送するためのサービス提供者側システム１と、コンテンツを再生するための多数の端末とから、構成されている。この端末には、パーソナルコンピュータ２，サービスクライアント６ａ，６ｂ，及びＤＶＤプレーヤ８が含まれている。また、パーソナルコンピュータ２にはリムーバブルディスク装置３が接続されている。また、第１のサービスクライアント６ａには、ＳＣＳＩインタフェースを介して光磁気ディスクドライブ４が接続されている。ＤＶＤプレーヤ８を除く各端末は、上位サービスレイヤインタフェースＳ１，及びアプリケーションサービスレイヤインタフェースＳ２を介して、サービス提供者側システム１に接続されている。

【００２２】これら上位サービスレイヤインタフェースＳ１，及びアプリケーションサービスレイヤインタフェースＳ２は、図２に示すＤＡＶＩＣ 1.0システムリファレンスモデルによって定義されたインタフェースである。この上位サービスレイヤインタフェースＳ１は、コンテンツを配送するためのインタフェースであり、具体的には、ケーブルテレビジョンシステムのケーブル，衛星回線，ＩＳＤＮ等である。また、アプリケーションサービスレイヤインタフェースＳ２は、アクセス制御情報を交換するためのインタフェースであり、ケーブルテレビジョンシステムのケーブル，ＩＳＤＮを上位サービスレイヤインタフェースＳ１と兼用することができる他、アナログ電話網を用いることができる。

【００２３】なお、図１に示した（Ｓ１）は、物理的運搬を意味する。即ち、サービス提供者から購入したコンテンツ入りのフロッピーディスクを運搬して、パーソナルコンピュータ１のリムーバブルディスク装置３にロードしたり、サービス提供者から購入したコンテンツ入りのビデオディスクを運搬して、ＤＶＤプレーヤ８にロードすることを意味する。このような物理的運搬も、Ｓ１のインタフェースに該当する。同様に、制御情報をＦＡＸ，メール等によって送信することも、Ｓ２のインタフェースに該当する。

【００２４】本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供者又はサービス提供者から提供される有料のコンテンツまたは機密情報を第三者から容易に傍受されることを防ぐ目的のために、サービス提供者側システム１とサービスクライアント６との間に、セキュリティ機構を設けた。このセキュリティ機構は、サービス提供者側システム１から供給されるコンテンツが第三者によって悪用されたり転用されることを防止するために、このコンテンツを暗号化してサービスクライアント６に提供する。即ち、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、図２に示したDAVIC 1.0システムリファレンスモデルに基づき、セキュリティ・アンド・アクセス・コントロール機能を、サービス提供者側システム１及びサービスクライアント６に置いたのである。

【００２５】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、サービスクライアント６に復号化機能を持たせるために、模倣や改造が難しいハードウェア機構を一部採用し、認証及び秘匿を実現した。

【００２６】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、ユーザへの利便性を考慮し、復号化機能を実現するアルゴリズム、鍵管理、認証、秘匿、および課金に関する情報などユーザのセキュリティに付随する機能を、利用者が携帯可能なモジュール（以後、「ＭＡＳＣ：Media Access and Security Card」と呼ぶ）５に収め、このＭＡＳＣ５をサービスクライアント６に脱着可能とした。そのた

め、このＭＡＳＣ５を何れかのサービスクライアント６に装着することにより、別個のサービスクライアント６であっても同様のサービスを享受することが可能となる。

【００２７】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、他の標準化作業を尊重するため、サービスクライアント６側の認証方式は、ISO/IEC9798-2 に準拠した。また、鍵管理方式は、B-MACスクランブル放送で採用されている方式に準拠した。また、暗号登録方式は、ISO/IEC 9979に準拠し、鍵サイズおよび入出力データサイズのみ規定するとともに処理アルゴリズムは規定しないものとした。また、ＭＡＳＣ５のサービスクライアント６との物理インタフェースは、DVB 方式案の一部を変更して採用した。

【００２８】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供形態の多様化（ケーブル、衛星システム、パッケージ等）に対応できるように、拡張性の高いデータ構造、処理方式を採用した。

【００２９】＜サービス提供者側システムの構成＞次に、図３を参照して、データ供給装置としてのサービス提供者側システム１の内部構成を説明する。図３に示すように、サービス提供者側システム１は、サーバ１０と、このサーバ１０と各々バス接続されたユーザプロファイル１１，第１データファイル１２，第２データファイル１３，デジタル署名部１４，認証部１５，鍵更新処理部１６，鍵管理部１８，及び乱数発生器２０と、サーバ１０に夫々接続された衛星回線Ｓ，ケーブルテレビジョンシステムのケーブルＣ，及び電話網Ｎと、鍵更新処理部１６に接続された鍵更新タイマ１７と、鍵管理部１８に接続されたサービスプロバイダＩＤ記憶部１９とから、構成されている。

【００３０】第１の送信手段及び第１の受信手段としてのサーバ１０は、サービス提供者側システム１全体の制御を行うとともに、衛星回線Ｓ，ケーブルテレビジョンシステムのケーブルＣ，電話網Ｎを介してサービスクライアント６と通信を行う処理装置である。

【００３１】ユーザプロファイル１１は、各ＭＡＳＣのＩＤが登録されているデータベースである。第１データファイル１２は、暗号化された多数のコンテンツ及びそれらのＩＤ（タイトルＩＤ）を格納するデータベースである。第２データファイル１３は、この第１データファイル１２に格納されていたコンテンツを別の鍵を用いて再暗号化したもの及びそれらタイトルＩＤを格納するデータベースである。即ち、これらのデータファイル１２，１３に格納されるコンテンツは、一定時間毎に再暗号化されて、一方のデータファイルから他方のデータファイルに移されるのである。なお、これらデータファイル１２，１３に格納されるコンテンツには、予めＭＰＥＧ－２規格により圧縮処理がなされている。

【００３２】ディジタル署名部１４は、ユーザに対する課金額に対応した一定範囲のコンテンツ再生を許可するデータを、このデータが正しいことを論理的に証明するデジタル署名情報を付して、サービスクライアント６に送信する部分である。

【００３３】認証部１５は、当該サービス提供者側システム１に対して通信を行ってきたサービスクライアントに装着された個々のＭＡＳＣ５がユーザプロファイル１１にそのＩＤが登録されているどのＭＡＳＣ５であるのかを調べる作業を行う。

【００３４】乱数発生手段としての乱数発生器２０は、この認証部１５の作業において用いられる乱数を発生する。鍵出力部としての鍵管理部１８は、認証部１５におけるＭＡＳＫの識別に用いる鍵（第１の鍵）を、ユーザプロファイル１１に登録されているＭＡＳＣのＩＤから生成するとともに、各データファイル１２，１３に格納されている暗号化されたコンテンツを復元するための鍵（第３の鍵）を、対応するタイトルＩＤに基づいて生成する。

【００３５】サービスプロバイダＩＤ記憶部１９は、この鍵管理部１８における鍵生成に用いられる当該サービス提供者側システムのＩＤ（サービスプロバイダＩＤ：ＩＤＰ）を保持しているメモリである。

【００３６】鍵更新処理部１６は、一方のデータファイル１２，１３に格納されているコンテンツを鍵管理部１８において生成されたタイトルＩＤに基づいて復元するとともに新たな鍵を作成し、復元されたコンテンツをこの新たな鍵によって暗号化して他方のデータファイル１２，１３に格納する。

【００３７】鍵更新タイマ１７は、この鍵更新処理部における処理のタイミングを規定するタイマである。

＜サービスクライアントシステムの構成＞次に、図４を参照して、サービスクライアントシステムの構成を説明する。

【００３８】図４に示すように、サービスクライアントシステムは、衛星回線からの電波を受信するパラボラアンテナ２２と、このパラボラアンテナ２２に接続された衛星デコーダ２３と、ケーブルテレビジョンシステムのケーブルに接続されたＣＡＴＶアダプタ２６と、光磁気ディスクドライブ４と、これら衛星デコーダ２３，ＣＡＴＶアダプタ２６，及び光磁気ディスクドライブ４に接続されたデータセレクタ３８と、このデータセレクタ３８に接続された本体部としてのサービスクライアント６と、このサービスクライアント６に装着されたモジュール部としてのＭＡＳＣ５と、電話網Ｎに接続されたモデム５７とから、構成されている。

【００３９】衛星デコーダ２３は、パラボラアンテナ２２によって受信された信号を復調する復調回路２４と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ２５とから、構成されている。デコーダ

２５の出力端子は、データセレクタ３８の第１コネクタに接続される。

【００４０】ＣＡＴＶアダプタ２３は、ケーブルから受信された信号を復調する復調回路２７と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ２８とから、構成されている。デコーダ２８の出力端子は、データセレクタ３８の第２コネクタに接続される。

【００４１】光磁気ディスクドライブ４は、データセレクタ３８の第４コネクタに接続されたエンコーダ３５と、このエンコーダ３５によってエラー訂正及びビットの並び替えがなされたデータを変調する変調回路３４と、光磁気ディスク３０に対してデータの書込／読み出しを行うピックアップ３１と、ピックアップ３１によって読み出されたデータを復調する復調回路３２と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ３３と、光磁気ディスク３０を回転させるとともにピックアップ３１をトラッキングさせるドライブ回路３６とから、構成されている。デコーダ３３の出力端子は、データセレクタ３８の第３コネクタに接続される。

【００４２】データセレクタ３８は、第１乃至第３コネクタから入力したデータを第４コネクタ又は第５コネクタに出力する。そのために、データセレクタ３８は、第１乃至第３の何れかのコネクタに接続線を接続するかを選択するスイッチＳＷ１と、第４又は第５の何れかのコネクタに接続線を接続するかを選択するスイッチＳＷ２とを備えている。

【００４３】サービスクライアント６は、データセレクタの第５コネクタに接続されたＤＬ４０，ホストＣＰＵ４１，及びスイッチ４２と、スイッチ４２に接続されたデマルチプレクサ４３と、このデマルチプレクサ４３に接続された画像用ＭＰＥＧ伸長回路４４と、この画像用ＭＰＥＧ伸長回路４４に接続されたＤ／Ａ変換器４７と、デマルチプレクサ４３に接続された音声用ＭＰＥＧ伸長回路４５と、この音声用ＭＰＥＧ伸長回路４５に接続されたＤ／Ａ変換器４８と、両ＭＰＥＧ伸長回路４４，４５に接続された同期回路４６と、ホストＣＰＵ４１に接続されたセクタペイロード対向テーブル４９と、モデム５７に接続されたインタフェース５０とから、構成されている。

【００４４】ＤＬ４０は、ディレイライン装置であり、トグルバッファ又はＦＩＦＯメモリから構成された帯域変換装置である。スイッチ４２はＣＰＵ４１からの指示に従い、データセレクタ３８からの信号線又はＭＡＳＣ５からの信号線をデマルチプレクサ４３に接続する。また、スイッチ４２は、ＣＰＵ４１からの指示に応じて、回路を開く。

【００４５】ホストＣＰＵ４１は、当該サービスクライアント６全体の制御を行う制御装置である。また、ホストＣＰＵ４１は、データセレクタ３８から受信したコンテンツが予め暗号化されているかどうかを解析する。そして、暗号化がなされていないのであればデータセレクタ３８からの信号線をデマルチプレクサ４３に接続させる指示をスイッチ４２に対して行い、暗号化がなされているのであればＭＡＳＣ５からの信号線をデマルチプレクサ４３に接続させる指示をスイッチ４２に対して行うとともに、ＭＡＳＣ５に対して復号化を指示する。なお、ホストＣＰＵ４１は、ＭＡＳＣ５の制御ＣＰＵ５１からの指示があった場合には、コンテンツが暗号化されている場合であっても、スイッチ４２に対してデータセレクタからの信号線をデマルチプレクサ４３に接続させる指示を行う。また、ホストＳＰＵ４１は、データサレクタ３８からコンテンツを構成する各フレームを受信する毎に、ＭＡＳＣ５に対して通知を行う。

【００４６】デマルチプレクサ４３は、コンテンツ中の音声データフレーム及び画像データフレームを分離する。そして、画像データフレームを画像用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４に出力し、音声データフレームを音声用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４５に出力する。

【００４７】ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４，４５は、ＭＰＥＧ規格で圧縮されたままの状態で送信されて来た画像データフレーム，又は音声データフレームを伸長して、画像又は音声を出力可能なフォーマットに復元する回路である。これらＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４，４５においてデータフレームの伸長をする際には、同期回路４６によって出力の同期がとられる。即ち、同期回路４６から出力される同期信号に同期して、各ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４，４５は、伸長されたデータフレームを出力するのである。

【００４８】画像用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４からの出力は、Ｄ／Ａ変換器４７によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアント２に接続されている図示せぬＴＶモニタ装置に向けて出力される。また、音声用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４５らの出力は、Ｄ／Ａ変換器４８によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアントに接続されている図示せぬスピーカに向けて出力される。

【００４９】セクタペイロード対応テーブル４９は、光磁気ディスク３０の各セクタとフレームとの関係を対応させているテーブルである。即ち、光磁気ディスクドライブ４からのコンテンツを読み出している場合において、ホストＣＰＵ４１によって各フレームが読みとられる毎に、このセクタペイロード対応テーブル４９によってセクタとの対応が調べられるのである。そして、現在のセクタから全てのフレームが読み出された時には、セクタコントローラ３７に対して、ピックアップ３１のトラッキングを行うべき旨が指示されるのである。

【００５０】第２の受信手段及び第２の送信手段としてのインタフェース５０は、モデム５７と電話網Ｎ（Ｓ２）を介して、サービス提供者側システム１のサーバ１０と通信を行い、制御情報の送受信を行う。

【００５１】次に、ＤＬ４０，ホストＣＰＵ５１，スイッチ４２，及びインタフェース５６に接続されるＭＡＳＣ５の説明を行う。サービスクライアント６に提供される各種コンテンツは、衛星通信の様に入手が容易な通信媒体を介して配送されることがあるので、その再生に対する課金方法を如何にするかが問題となる。また、このような通信媒体を介して配送されるコンテンツは第三者による盗用を防止するために予め暗号化された状態で流通されるので、これを復号化する必要がある。そのため用いられるのがＭＡＳＣ５である。即ち、ＭＡＳＣ５は、ホストＣＰＵ４１からの指示に応じて、ＤＬ４０を介して受信したコンテンツを復号化してスイッチ４２に送信する。また、ＭＡＳＣ５は、ホストＣＰＵ４１がフレーム４１を受信する毎に行う通知をカウントして、課金カウンタ値Ｘを減算する。この課金カウンタ値Ｘとは、ユーザがサービス提供者側システムのデジタル署名部１４に対して代金支払いを了承することによって当該ＳＤ回路に書き込まれたポイントである。ＭＡＳＣ５は、この課金カウンタ値Ｘが０になった時に、ホストＣＰＵ４１に対して、スイッチ４２を開かせるのである。

【００５２】なお、このＭＡＳＣ５は、サービスクライアント６のカードスロット（たとえばＰＣＭＣＩＡ準拠のカードスロット）内に着脱自在に装着されたＩＣカードの形態で実現される。このようなＩＣカードの形態にしておけば、ＳＤ回路の運搬が容易となる。

【００５３】このＭＡＳＣ５は、相互にバス接続された制御ＣＰＵ５１，ＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）５３，課金情報記憶部５５，ＲＯＭ５７，並びにＩ／Ｏ装置５２，５４，及び５６から構成されている。

【００５４】制御ＣＰＵ５１は、サービスクライアント６内のホスト制御ＣＰＵ１４に接続されており、ホストＣＰＵ４１からの指示に応じてＤＥＳ５３に対して復号化処理を実行させる。また、制御ＣＰＵ５１は、ホストＣＰＵ４１からのフレーム受信通知に応じて課金部５５内に格納されている課金カウンタ値Ｘを減算するとともに、この課金カウンタ値Ｘが０になったときは、ＣＰＵ４１に対して、スイッチ４２を開かせる。また、制御ＣＰＵ５１は、Ｉ／Ｏ装置５６，インタフェース５０及びモデム５７を介してサービス提供者側システム１との間で通信を行って、アクセス要求，ディジタル署名，及びユーザ認証のために必要な処理を行う（アクセス要求手段に対応）。

【００５５】鍵保持手段としてのＲＯＭ５６は、この制御ＣＰＵ５１における処理に必要な諸データ（例えば、当該ＭＡＳＣ５を識別するための識別ＩＤ$_i$［固有の識別情報］，当該ＭＡＳＣ５に固有のものとして備えられた個別鍵Ｋ$_i$［第２の鍵］）を記憶しているメモリである。

【００５６】課金情報記憶部５５は、上述した課金カウンタ値Ｘを格納しているメモリである。なお、課金情報記憶部５５内において、課金カウンタ値Ｘは暗号化されている。従って、ユーザがこの課金情報記憶部５５を解析して課金カウンタ値Ｘを書き換えることは、不可能である。

【００５７】第２の暗号化手段，並びに第１及び第２の複合化手段としてのＤＥＳ７は、Ｉ／Ｏ装置５２を介してＤＬ４０から受け取ったコンテンツを復号化する機能，及び制御ＣＰＵ５１が行うディジタル署名及びユーザ認証に際して必要な暗号化及び復号化を行う機能を有する。ＤＥＳ７により復号化されたコンテンツ（画像フレーム，音声フレーム）は、Ｉ／Ｏ装置５４を通じて、スイッチ４２に送出される。

《実施例における処理内容》次に、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいて、サービス提供者側システム１とサービスクライアント６との間で実行される制御処理を、フローチャート及びこのフローチャートの各ステップにおいて実現される機能を示すための機能ブロック図を参照して、説明する。

【００５８】サービスクライアント６がサービス提供者側システム１管理の情報にアクセスする場合、安全な通信制御手段が必要となる，これはサービスクライアント６とサービス提供者側システムとの間を結ぶＳ１とＳ２の形態により異なる。

【００５９】（コンテンツ情報送信制御処理）先ず最初に、サービスクライアント６側からサービス提供側システム１に対して何れかのコンテンツの配送を要求する際の制御処理について説明する。この場合、Ｓ１，Ｓ２のインタフェースが秘密保持性が高い通信媒体であるか否かによって、制御を異にする。なぜならば、秘密保持性が低い通信媒体によってコンテンツを配送する場合には、第三者による盗用やデータ改ざんを防ぐために暗号化する処理が不可欠だからである。

【００６０】＜秘密保持性が高い通信媒体によるコンテンツ情報供給制御＞図５は、Ｓ１，Ｓ２の形態を、例えば光ファイバケーブル（ケーブルテレビジョンシステムのケーブル，等）のように、データ盗聴やデータ改ざんが比較的困難な信頼できるネットワークとした場合における制御内容を示す，この場合、サービスクライアント６側の不正アクセスのみが問題となる。従って、アクセス権確立のための認証が重要となる，

【００６１】この場合の運用手順の概略を説明すると、最初にユーザは、サービスクライアント６にＭＡＳＣ５を挿入する。すると、サービスクライアント６は、ＭＡＳＣ５の識別ＩＤ（ＩＤ$_i$）を読み取り、その識別ＩＤ

（ＩＤi）をサービス提供者側システムへ通知する。すると、サービス提供者側システム１は、何れのＭＡＳＣ５であるかを認証する。次に、サービス提供者側システム１は、要求されたコンテンツをサービスクライアント６に向けて配送し、課金システムを動作させる。その結果、サービスクライアント６は、コンテンツを入手する。

【００６２】［アクセス要求］図５における最初のステップ０１では、サービスクライアント６は、サービス提供者側システム１に対してアクセス要求を行う。この前提として、サービスクライアント６が所有するＭＡＳＣ５には、モジュール固有の識別ＩＤ（ＩＤi），個別鍵Ｋi，及び認証アルゴリズムＥＫ(X)が安全に格納されている。

【００６３】ユーザは、このＭＡＳＣ５を任意のサービスクライアント６へ接続し、図示せぬ操作キーを介してサービス提供者側システムの識別ＩＤ（サービスプロバイダＩＤ：ＩＤp）を入力する。すると、図６（１）に示すように、サービスクライアント６は、サービス提供者側システムへのデータファイルアクセス要求コマンド，及びモジュール固有の識別ＩＤに、サービス提供者側システムのデスティネーション〔サービス提供者側システムの識別ＩＤ（ＩＤp）とサービスクライアント６の識別ＩＤ（アドレス）とを結合したもの〕を付して、Ｓ２インタフェースを介してサービス提供者側システム１に送信する。なお、この時、サービスクライアント５は、配送を求めるコンテンツのタイトルＩＤ（ＩＤＴ）を、サービス提供者側システム１に送信する。

【００６４】［認証処理］図５における次のステップ０２では、サービス提供者側システム１によるサービスクライアントの認証処理を行う。このサービスクライアント認証は、当事者以外の第三者によるサービス提供者側システム１のデータファイルへの不正アクセス阻止を目的に実行される。ここでは、ISO/IEC 9798-2を利用し、当事者間で互いに共有する秘密の鍵データが同一であることにより認証を行う。

【００６５】サービス提供者側システム１がアクセス要求をしたサービスクライアント６の正当性を認証する場合には、図６に示すような手順で認証処理を行う。尚、この認証のための通信は、Ｓ２インタフェースを介して行われる。

【００６６】サービス提供者側システム１のサーバ１０がサービスクライアント６からのアクセス要求を受信すると（１）、鍵管理部１８内の第１鍵生成部（鍵出力部）１８２は、受信したＭＡＳＣ識別ＩＤ（ＩＤi）がユーザプロファイル１１に登録されていることを確認し、ユーザプロファイル１１内の当該識別ＩＤ（ＩＤi）を基に、プロバイダ管理の第１マスタ鍵８１を使ってクライアント個別鍵（第１の鍵）Ｋiを生成する。この第１マスタ鍵８１は、ＭＡＳＣ５内に格納されている個別鍵（第２の鍵）Ｋiが生成された際に用いられたマスタ鍵と同一である。従って、受信したＭＡＳＣ識別ＩＤ（ＩＤi）とユーザプロファイル１１内に登録されている識別ＩＤ（ＩＤi）とが同一である限り、ＭＡＳＣ５内の個別鍵Ｋiと全く同じクライアント個別鍵Ｋiが生成されることになる。

【００６７】これと同時に、サービス提供者側システム１内の乱数発生部２０は、乱数Ｒを発生する。この乱数Ｒは、認証部１５に入力されるとともに、サーバ１０にも入力される。サーバ１０は、この乱数Ｒにサービスクライアント向けデスティネーション〔サービスクライアント６の識別ＩＤ（アドレス）とサービス提供者側システムの識別ＩＤ（ＩＤＰ）とを結合したもの〕を付けて、サービスクライアント６へ送信する（２）。

【００６８】サービス提供者側システム１からの情報を受信したサービスクライアント６は、情報に含まれる乱数ＲをＭＡＳＣ５に与える。すると、ＭＡＳＣ５は、ＭＡＳＣ識別ＩＤ（ＩＤi）に乱数Ｒを結合して、これを個別鍵Ｋiによって暗号化することにより、第２の認証子を生成する。サービスクライアント６は、この第２の認証子にサービス提供者側システムのデスティネーションを付して 再びサービス提供者側システム１へ送り返す（３）。

【００６９】このクライアント情報を受信したサービス提供者側システム１は、この情報に含まれる第２の認証子を、認証部１５内の比較器（比較手段）１５２へ設定する。更に、認証部１５内の第１暗号化部（第１の暗号化手段）１５１は、サービスクライアント５から受信したＭＡＳＣ識別ＩＤと乱数発生部２０から受信した乱数Ｒとを結合して、これを鍵生成部１８２にて生成されたクライアント個別鍵Ｋiによって暗号化することにより、第１の認証子を生成する。第１暗号化部１５１は、この第１の認証子を比較器１５２へ設定して、先に設定した第２の認証子と比較させる。比較器１５２において両認証子が一致すれば、サービスクライアント５及びサービス提供者側システム１間に同一の個別鍵Ｋiが保有されていることになるので、認証部１５は、当該サービスクライアントを通信当事者として認証し、後の処理を可能とする。これに対して、両認証子が相違している場合には、そのＭＡＳＣ５に対応する課金用データが登録されていないサービスクライアントであると判断して、後の処理を禁止する。　このように、本実施例による認証方式によると、認証の対象となる個別鍵Ｋi自体がインタフェース上を送信されるのではなく、アクセス要求の都度生成される乱数をこの個別鍵Ｋiで暗号化した認証子が送信されるだけである。従って、第三者が乱数Ｒを盗んだとしても、個別鍵Ｋiの内容を知らない限り、認証子を生成することは不可能である。また、認証子自体を盗んだとしても、既に正規のユーザに対する認証が済んでいる場合には、この認証子に対する乱数Ｒは認証

部１５にセットされていないので、当該認証子は既に無効となっている。このように何れにしても第三者の不正なアクセスは、阻止されるのである。

【００７０】なお、サービスクライアント６がサービス提供者側システム１を認証するときには、上記のサービスクライアント６及びサービス提供者側システム１の立場を入れ換えて同様な手順を実行することにより、サービスクライアント６がサービス提供者側システム１を認証することが可能となる。

【００７１】また、認証プロセスで用いるパラメータは、認証子の生成アルゴリズムにより異なる。例えば生成アルゴリズムにＤＥＳ(DATA ENCRYPTION STANDARD)を採用した場合，以下の通りである。

【００７２】

乱数Ｒ　　：32 ビット

ＭＡＳＣ識別ＩＤ：32 ビット(ＥＣＢ入力時には残り32ビットはパディングする)

個別鍵K_i　　：56 ビット

マスタ鍵ＫＭ　　：168ビット(56 ビット×3)

サービス提供者側システム１の利用モード：TRIPPLE ECB(ELECTRONIC CODE BOOK)(個別鍵生成，乱数生成)

サービスクライアントの利用モード：ECB(認証処理)

［コンテンツ情報配送処理］図５における次のステップ０３では、サービスクライアント６からのコンテンツ情報配送処理を行う。即ち、サービス提供者側システム１は、サービスクライアント５から要求されたタイトルＩＤ（ＩＤＴ）に対応するコンテンツ（暗号化コンテンツ）を、何れかのデータファイル１２，１３から読み出して復号化する。そして、Ｓ１インタフェースを介して、復号化されたコンテンツをサービスクライアント６に送信するのである。

【００７３】コンテンツを受け取ったサービスクライアント６は、これを一旦光ディスクドライブ４に送信して光ディスク３０に書き込むか、そのままＣＰＵ４２に流す。ホストＣＰＵ４２はこのコンテンツが暗号化されていないものであると解析して、スイッチ４３をデータセレクタ側に切り換える。従って、コンテンツはそのままデマルチプレクサ４３にて画像フレームと音声フレームに分離されて、夫々ＭＰＥＧ伸長回路４４，４５にて伸長され、ＤＡ変換器４７，４８にてアナログ信号に変換される。そして、画像信号は図示せぬＴＶモニタへ送信され、音声信号は図示せぬスピーカへ送信される。

【００７４】また、ホストＣＰＵ４１は、コンテンツを構成する各フレームを読み込む毎に、ＭＡＳＣ５内の制御ＣＰＵ５１に通知を行う。この制御ＣＰＵ５１は、通知の数をカウントして、課金情報記憶部５５内の課金カウント値Ｘを減算する。そして、この課金カウント値Ｘが０になると、制御ＣＰＵ５１は、ホストＣＰＵ４１に対して、スイッチを４２を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止されるのである。

【００７５】<一般のネットワークによるコンテンツ情報供給制御>図７は、Ｓ１，Ｓ２の形態を、無線路や様々な迂回路を経由する一般のネットワーク形態とした場合における制御内容を示す。この形態では、データ盗聴やデータ改ざん行為が十分起こり得るので、上述のサービスクライアント認証処理の他、データ暗号化を如何に行うかが重要である.

【００７６】この場合の運用手順の概略を説明すると、最初に利用者は、サービスクライアント６にＭＡＳＣ５を挿入する。すると、サービスクライアント６は、ＭＡＳＣ５の識別ＩＤ（ID_i）を読み取り、その識別ＩＤ（ID_i）をサービス提供者側システムへ通知する。すると、サービス提供者側システム１は、何れのＭＡＳＣ５であるかを認証する。次に、サービス提供者側システム１は、サービスに必要な鍵（KG_j）をサービスクライアント６に配送する。このようにして、サービスクライアント６は、必要な鍵（KG_j）を入手する。その後、サービス提供者側システム１は、要求されたコンテンツをサービスクライアント６に向けて配送し、課金システムを動作させる。その結果、サービスクライアント６は、この鍵（KG_j）を利用してコンテンツを入手する。

【００７７】［アクセス要求］図７における最初のステップ１１では、サービスクライアント６は、図８に示すように、サービス提供者側システム１に対してアクセス要求を行う。このアクセス要求の内容は、図５におけるステップ０１と同じなので、その説明を省略する。

【００７８】［認証処理］図７における次のステップ１２では、サービス提供者側システム１は、図８に示すように、サービスクライアント６の認証を行う。この認証処理は、図５におけるステップ１２と同じなので、その説明を省略する。

【００７９】［鍵配送処理］図７における次のステップ１３では、サービス提供者側システム１は、図８に示すように、暗号化コンテンツの復元用の鍵（KG_j）の配送を行う。この鍵配送は、暗号化されている各種コンテンツの情報をサービスクライアント６側で円滑に復号させる為に、Ｓ２インタフェースを使って行われる。

【００８０】即ち、サービス提供者側システム１は、サービスクライアント６に装着されたＭＡＳＣ５が発信してきたＭＡＳＣ識別ＩＤ（ID_i）から、クライアント個別鍵K_iを生成しする（このクライアント個別鍵K_iとしてクライアント認証において用いたものを流用しても良い。）。サービス提供者側システム１は、クライアント個別鍵K_i鍵によってサービスプロバイダＩＤ（ＩＤＰ）及びタイトル鍵KG_{1j}を暗号化し、サービスクライアント向けデスティネーション〔サービスクライアント６の識別ＩＤ（アドレス）とサービス提供者側システムの識別ＩＤ（アドレス）とを結合したもの〕を付して、

ＭＡＳＣ５に送信する。サービス提供者側システム１からの暗号化鍵情報は、ＭＡＳＣ５において復号化され、タイトル鍵KG_{1j}が得られる。以後、Ｓ１インタフェースで送られてくる暗号化コンテンツが、このタイトル鍵KG_jによって復号化される。

【００８１】この鍵配送処理の内容を、図９の機能ブロック及び図１０のサブルーチンフローチャートに基づいて説明する。なお、説明の都合上、現時点において第１データファイル１２に暗号化コンテンツが格納されているとし、これを「旧データファイル」と称するものとする。

【００８２】図１０において、最初のステップ２１では、サービス提供者側システム１の鍵管理部１８内に備えられたスイッチＳＷ４を、旧データファイル１２側に切り換える。そして、サービスクライアント５から要求されているタイトルに対応するタイトルＩＤ（ＩＤＴ）を、スイッチＳＷ４を介して旧データファイル１２から読み出す。第２鍵生成部１８４は、読み出したタイトルＩＤ（IDT_j）を第２マスタ鍵１８５に基づいて暗号化し、タイトル鍵（第３の鍵）KG_{1j}を生成する。

【００８３】次のステップ２２では、鍵管理部１８内の第２暗号化部（第３の暗号化手段）１８３は、サービスプロバイダＩＤ記憶部１９から受信したサービスプロバイダＩＤ（ＩＤＰ）と、第２鍵生成部１８４から受信したタイトル鍵KG_jとを、結合する。そして、第２暗号化部１８３は、認証処理時において第１鍵生成部１８２が生成したクライアント個別鍵K_iに基づいて、これらサービスプロバイダＩＤ（ＩＤＰ）及びタイトル鍵KG_{1j}を暗号化し、サーバ１０に転送する。サーバ１０は、受け取ったサービスプロバイダＩＤ及びタイトル鍵KG_{1j}の暗号化情報を、Ｓ２インタフェースを介してサービスクライアント６に配送する。

【００８４】次のステップ２３では、サービスクライアント６は、サービスプロバイダＩＤ及びタイトル鍵KG_{1j}の暗号化情報をＭＡＳＣ５に配送する。ＭＡＳＣ５内の第１復号化部（第２の複合化部）１０１（ＤＥＳ５３）は、ＭＡＳＣ６のＲＯＭ５７に内蔵されている個別鍵K_iを用いてこの暗号化情報を復号化し、サービスプロバイダＩＤ及びタイトル鍵KG_{1j}を獲得する。そして、このサービスプロバイダＩＤ（ＩＤＰ）を比較器１０２にセットする。

【００８５】次のステップ２４では、ＭＡＳＣ６内の比較器１０２は、第１復号化部１０１によってセットされたサービスプロバイダＩＤ（ＩＤＰ）とアクセス要求時に図示せぬ操作キーを介して入力されたサービスプロバイダＩＤ（ＩＤＰ）１０３とを、比較する。そして、両者が一致している場合には、処理をステップ２５に進め、不一致の場合には、処理をステップ２７に進める。

【００８６】ステップＳ２７において、受信不可能である旨がサービスクライアント５側に通知され、Ｓ２インタフェースを介してサービス提供者側システム１のサーバ１０に転送される。

【００８７】次のステップ２８では、サービス提供者側システム１のサーバ１０は、第２暗号化部１８３から受け取ったサービスプロバイダＩＤ（ＩＤＰ）及びタイトル鍵KG_{1j}の暗号化情報を、Ｓ２インタフェースを介して再度ＭＡＳＣ５側へ配送する。その後、処理はステップＳ２３に戻される。

【００８８】これに対して、ステップ２５では、ＭＡＳＣ６内のスイッチＳＷ３が閉じられ、第１復号化部１０１において復元されたタイトル鍵KG_{1j}が第２復号化部（第１の復号化手段）１０４（ＤＥＳ５３）にセットされる。それとともに、受信可能である旨がサービスクライアント５側に通知され、Ｓ２インタフェースを介してサービス提供者側システム１のサーバ１０に転送される。

【００８９】ステップ２６において、サービス提供者側システム１のサーバ１０は、スイッチＳＷ１を閉じて、データファイル１２からタイトル鍵KG_{1j}に対応するタイトルの暗号化コンテンツを読み出す。

【００９０】［コンテンツ情報配送処理］図７のステップ１４において実行されるコンテンツ情報配送処理は、図１０のステップ２６の直後に実行される。

【００９１】即ち、図１１に示すように、サーバ１０は、データファイル１２から読み出した暗号化コンテンツを、Ｓ１インタフェースを介してサービスクライアント６に配送する。サービスクライアント６は、この暗号化コンテンツをＭＡＳＣ５に転送する。ＭＡＳＣ５の第２復号化部１０４（ＤＥＳ５３）は、セットされたタイトル鍵KG_{1j}を用いてこの暗号化コンテンツを復号化する。

【００９２】図４を用いてこの復号化を具体的に説明する。コンテンツを受け取ったサービスクライアント６は、これを一旦光ディスクドライブ４に送信して光ディスク３０に書き込むか、そのままＣＰＵ４２に流す。ホストＣＰＵ４２はこのコンテンツが暗号化されているものであると解析して、スイッチ４３をＭＡＳＣ側に切り換えるとともに、ＭＡＳＣ５の制御ＣＰＵ５１に対して、復号化処理を指示する。この指示に応じて、制御ＣＰＵ５１は、暗号化コンテンツをＤＬ４０及びＩ／Ｏ装置５２を介して読み込み、ＤＥＳ５３（第１復号化部１０１，第２復号化部１０４）によって復号化を行う。このＤＥＳ５３には、インタフェース５０及びＩ／Ｏ装置５６を介して受信したタイトル鍵KG_{1j}がセットされているので、このタイトル鍵KG_{1j}を用いて複合化する。複合化されたコンテンツは、Ｉ／Ｏ装置５４を介してスイッチ４２に送信される。

【００９３】コンテンツは、スイッチ４２からデマルチプレクサ４３に転送され、このデマルチプレクサ４３にて画像フレームと音声フレームに分離されて、夫々ＭＰ

ＥＧ伸長回路４４，４５にて伸長され、ＤＡ変換器４７，４８にてアナログ信号に変換される。そして、画像信号は図示せぬＴＶモニタへ送信され、音声信号は図示せぬスピーカへ送信される。

【００９４】また、ホストＣＰＵ４１は、コンテンツを構成する各フレームを読み込む毎に、ＭＡＳＣ５内の制御ＣＰＵ５１に通知を行う。この制御ＣＰＵ５１は、通知の数をカウントして、課金情報記憶部５５内の課金カウント値Ｘを減算する。そして、この課金カウント値Ｘが０になると、制御ＣＰＵ５１は、ＤＥＳ５３による復号化を中止するとともに、ホストＣＰＵ４１に対してスイッチを４２を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止されるのである。

【００９５】このように、本実施例のキー配送処理によれば、データファイル１２に格納されている各コンテンツ毎に、別個の復元用鍵（タイトル鍵KG_{1j}）を生成した。従って、同一のユーザが同じキーを用いて他のタイトルのコンテンツを再生することが防止できる。また、このタイトル鍵KG_{1j}は、ＭＡＳＣ５毎に用意された鍵（個別鍵K_j）によって暗号化されるので、第三者が暗号化された鍵を傍受したとしても、タイトル鍵KG_{1j}を復元することは不可能である。従って、第３者の盗用が阻止できる。

【００９６】（ローカル課金処理）次に、コンテンツ情報を再生するために必要な課金カウント値Ｘの加算を申込むためのローカル課金処理を、図１２に基づいて説明する。この課金カウント値Ｘの加算値は、サービスクライアント６からサービス提供者側システム１に対して、代金の銀行口座からの引き落としを条件に申し込まれ、サービス提供者側システム１によってＭＡＳＣ５に書き込まれる。このように、本実施例では、課金カウント値Ｘの管理をＭＡＳＣ５において行っているので、特にデータ改ざん防止に重点が置かれる。よって、サービス供給者側システム１がこの加算値の正当性を証明するために加算値情報に付すデジタル署名が重要となる。従って、サービス提供者側システム１には、予め、ＭＡＳＣ５毎に、暗証番号が登録されているものとする。

【００９７】［アクセス要求］図１２における最初のステップ３１では、サービスクライアント６は、図１３に示すように、サービス提供者側システム１に対してアクセス要求を行う。このとき、サービスクライアント６は、サービス提供者側システム１への課金カウント値増加要求コマンド，及びＭＡＳＣ固有の識別ＩＤに、サービス提供者側システムのデスティネーション〔サービス提供者側システムの識別ＩＤ（サービスプロバイダＩＤ：ＩＤＰ）とサービスクライアント６の識別ＩＤ（アドレス）とを結合したもの〕を付して、Ｓ２インタフェースを介してサービス提供者側システム１に送信する。

【００９８】［認証処理］図１２における次のステップ３２では、サービス提供者側システム１は、図１３に示すように、サービスクライアント６の認証を行う。この認証処理は、図５におけるステップ０２と同じなので、その説明を省略する。

【００９９】［デジタル署名処理及び課金カウント値の書込処理］図１２における次のステップ３３では、サービスクライアント６においてデジタル署名が行われ、次のステップＳ３４では、サービス提供者側システム１による課金カウント値Ｘの補充処理が行われる（図１３参照）。

【０１００】即ち、ユーザによるメッセージの認証は、サービス提供者側システム１とサービスクライアント５との間で、課金に関わるセンシティーブデータをやりとりするときに、通信路上での第三者によるデータの改竄行為やサービスクライアント６でのユーザによるデータ改竄行為を阻止し、当事者間で円滑なトランザクション行為を達成するために、用いられる。ここでは、ISO 8731-1に基づくＭＡＣ(MESSAGE AUTHENTICATION CODE)方式を利用する。

【０１０１】サービス提供者側システム１のデジタル署名部１４は、ユーザの銀行口座から引き落とす金額に対応する補充カウンタ値のデータブロック（DATA OF MENEY）１４０を、送信用フレームＦに格納する。補充カウンタ値のデータブロック（DATA OF MENEY）１４０は、また、当該ＭＡＳＣ５についての加算履歴回数に応じてインクリメントされる通番（ＩＶ）によって署名処理される（ステップ３３）。即ち、排他ＯＲ回路１４２及び第３暗号化部１４３において、暗証番号（ＩＶ）を用いて、補充カウンタ値のデータブロック（DATA OF MENEY）１４０が暗号化されるのである。このような署名処理の最終処理結果（ＭＡＣ）は、サービス提供者側システム１が補充カウンタ値の正当性を証明するためのデータとして、送信用フレームＦに格納される。この送信用フレームＦは、Ｓ２インタフェースを介して、サービスクライアント６に装着されたＭＡＳＣ５に送信される（ステップ３４）。

【０１０２】ＭＡＳＣ５は、受信した送信用フレームＦに対して、サービス提供者側システム１側と同一処理を行う。即ち、送信用フレームＦから補充カウンタ値のデータブロック（DATA OF MENEY）１４０を読み出す。そして、排他ＯＲ回路１０６及び暗号化回路１０６（ＤＥＳ５３）において、補充履歴回数に応じてインクリメントされる通番（ＩＶ）を用いて、補充カウンタ値データブロックの全てに対して署名処理を行う。なお、この通番（ＩＶ）は、通常であれば、サービス提供者側システム１のディジタル署名部１４に格納されている通番（ＩＶ）に同期している。次に、比較器１０７において、署名処理の結果生成されたＭＡＣの値（ＭＡＣ’）と送信用フレームＦに格納されたＭＡＣ１４１の値とを比較する。比較の結果、両値が一致した時には、送信用フレー

ムFに格納された補充カウンタ値のデータブロック（DATA OF MENEY）１４０が正しい金額データであると判断し、スイッチＳＷ６を閉じる。すると、この補充カウンタ値が、課金情報記憶部５５に格納されている課金カウンタ値Ｘに加算される。

【０１０３】以上の結果、ユーザが送信用フレームＦから補充カウンタ値を読み出してこれを書き換えた場合には、この書き換えた補充カウント値が課金カウント値Ｘに加算できなくなってしまうので、不正が防止できる。

【０１０４】このデジタル署名処理に用いられるパラメータは以下の通りである。

暗号化処理　：DES
署名鍵　：56ビット
ＭＡＣ　：32ビット(64 ビット出力の左32ビットを抽出)
金額データ　：64ビットブロック単位(不足分の32ビットはパディングビットを挿入)

（鍵の更新処理）次に、一定時間毎に、旧データファイル１２に格納されたコンテンツを新規なタイトル鍵KG_{2j}によって暗号化し直して新データファイル１３に格納するための処理を図９のブロック図及び図１４のフローチャートを参照して説明する。

【０１０５】即ち、サービス提供者側システム１で管理する各種タイトルのコンテンツは、それぞれのタイトル鍵KG_{1j}で予め暗号化されているが、同一の鍵で恒久的に暗号化した場合、解読の危険性が高まる。この為、タイトル鍵KG_1の定期的更新を行って、暗号化をし直す必要があるのである。また、新たに追加されたタイトルのコンテンツに対しても、その都度タイトルに応じたタイトル鍵KG_{2j}で暗号化する必要がある。そのため、本実施例では、データファイルを第１のデータファイル１２及び第２のデータファイル１３に分け、一方のデータファイルに現在稼働中の暗号化情報を格納するとともに（旧データファイル）、他方のデータファイルには図１４の鍵の更新処理を実行することにより新たな暗号化コンテンツを格納するのである（新データファイル）。この図１４の処理の前提として、鍵管理部１８の第２マスタキー１８５と鍵更新処理部１６の第２マスタ鍵１６３とは全く同じものであるとする。また、一度使用したタイトル鍵KG_{1j}は再使用を行うことなく使い捨てられるので、タイトル鍵KG_{1j}の生成に用いられる第２マスタ鍵１６３，１８５は、鍵更新の都度変更される。

【０１０６】図１４の処理は鍵更新タイマ１７に設定された周期毎にスタートする。即ち、本実施例では、タイトル鍵KG_{1j}の更新を、プログラムのサイクル及び安全係数を考慮に入れ、例えば一週間毎に行うようにしている。なお、図１４の処理のスタートタイミング，即ち、新タイトル鍵KG_{2j}によって暗号化され直した新コンテンツの新データファイルへ格納するタイミングは、旧データファイル稼働中であることは、言うまでもない。また、第１データファイル１２を旧データファイルとする場合には、スイッチＳＷ１を閉じ、スイッチＳＷ２を開き、スイッチＳＷ４を第１データファイル１２側とし、スイッチＳＷ５を第２データファイル側１３とする。これに対して、第２データファイル１３を旧データファイルとする場合には、これらと全く逆にする。

【０１０７】図１４の処理において最初のステップ４１では、鍵更新処理部１６の復号処理部（第３の復号化手段）１６１に、第２鍵生成部１８４において現在のタイトルＩＤ（IDT_{1j}）に基づいて生成されたタイトル鍵KG_1をセットする。

【０１０８】次のステップ４２では、旧データファイル１２に格納されている当該タイトル鍵KG_1に対応する暗号化コンテンツを鍵更新処理部１６の復号装置１６１にセットして、タイトル鍵KG_1に基づいて復号を行う。

【０１０９】次のステップ４３では、鍵更新処理部１６の第３鍵生成部（鍵更新手段）１６４は、新データファイルに予め格納されている何れかのタイトルＩＤ（IDT_{2j}）を第２マスタ鍵１６３により暗号化して、新タイトル鍵KG_{2j}を生成する。第４暗号化部（第３の暗号化手段）１６２は、復号されたコンテンツを新タイトル鍵KG_{2j}に基づいて暗号化し直す。

【０１１０】次のステップ４４では、第４暗号化部１６２が暗号化し直した暗号化コンテンツを、新データファイル１３に書き込む（書込手段に対応）。次のステップ４５では、鍵更新タイマー１７によってある期限（例えば毎日曜日の深夜以降）まで待ち、各スイッチＳＷ１，２，４，５を切り換える。例えば、第１データファイルを旧ファイルとしていた場合においては、スイッチＳＷ２を閉じ、スイッチＳＷ１を開き、スイッチＳＷ４を更新側に切り換え、スイッチＳＷ５を旧データファイル１２側に切り換える。これより、新データファイル１３に格納されているタイトルＩＤ（IDT_{2J}）を鍵管理部１８に送信可能となり、新データファイル１３に格納されている暗号化コンテンツをサーバ１０に送信可能となるとともに、この新データファイルを旧データファイルとして扱う次回の更新処理が可能となる。このステップ４４の処理が完了すると、処理が図１０のステップ２１に渡される。

【０１１１】（MASC の緊急対策）ユーザ側で万一ＭＡＳＣ５の紛失又は盗難に遭遇した場合、サービス提供者は、緊急に鍵の破壊及びＭＡＳＫ５の再発行を行う。即ち、ユーザは、ＭＡＳＣ５の紛失又は盗難の事実が確認されたなら、電話等の通信手段を使って直ちにサービス提供者にそのむね連絡する。このときユーザは、自身の名前，住所，連絡先をサービス提供者に通知する。次に、サービス提供者は、サービス提供者側システム１のプロファイルデータでユーザを確認後、ユーザに対して電話によるコールバックを行う。そして、サービス提供

者及びユーザ間で確認及び合意がとれれば、サービス提供者は、プロファイルから該当ユーザデータ全てを抹消し、対応するＭＡＳＣ５のＩＤ（ＩＤi）を永久欠番とする。その後、ユーザは、サービス提供者又は近くの特約店或いは代理店へ行き、再登録の申請を行い、新しいＩＤ（ＩＤi）付ＭＡＳＣ５を発行してもらう。

【０１１２】

【発明の効果】以上のように構成された本発明のクライアント認証システムの第１の態様によると、ユーザ（クライアント）とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方おいて動的に作成するので、第三者の盗用が不可能となる。

【０１１３】また、本発明のクライアント認証システムの第１の態様によると、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着されるモジュールに、認証を行うためのデータ及び機能を持たることができるので、再生装置が自己のものか否かに拘わらずコンテンツを再生できるとともに、サービス提供者は確実にコンテンツ再生代金を徴収することができる。

【図面の簡単な説明】

【図１】　本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図

【図２】　図１のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図

【図３】　図１のサービス提供者側システムの構成を示すブロック図

【図４】　図１のサービスクライアント側システムの構成を示すブロック図

【図５】　秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート

【図６】　認証処理に関連する構成を示すブロック図

【図７】　一般のネットワークによるコンテンツ情報供給制御を示すフローチャート

【図８】　鍵配送処理を示すタイムアロー図

【図９】　鍵配送処理に関連する構成を示すブロック図

【図１０】　鍵配送処理の内容を示すフローチャート

【図１１】　コンテンツ配送処理を示すタイムアロー図

【図１２】　ローカル課金処理の内容を示すフローチャート

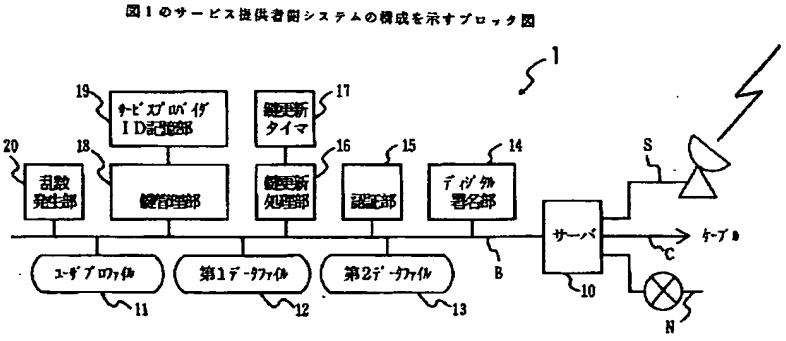
【図１３】　デジタル署名処理に関連する構成を示すブロック図

【図１４】　鍵の更新処理の内容を示すタイムアロー図

【符号の説明】

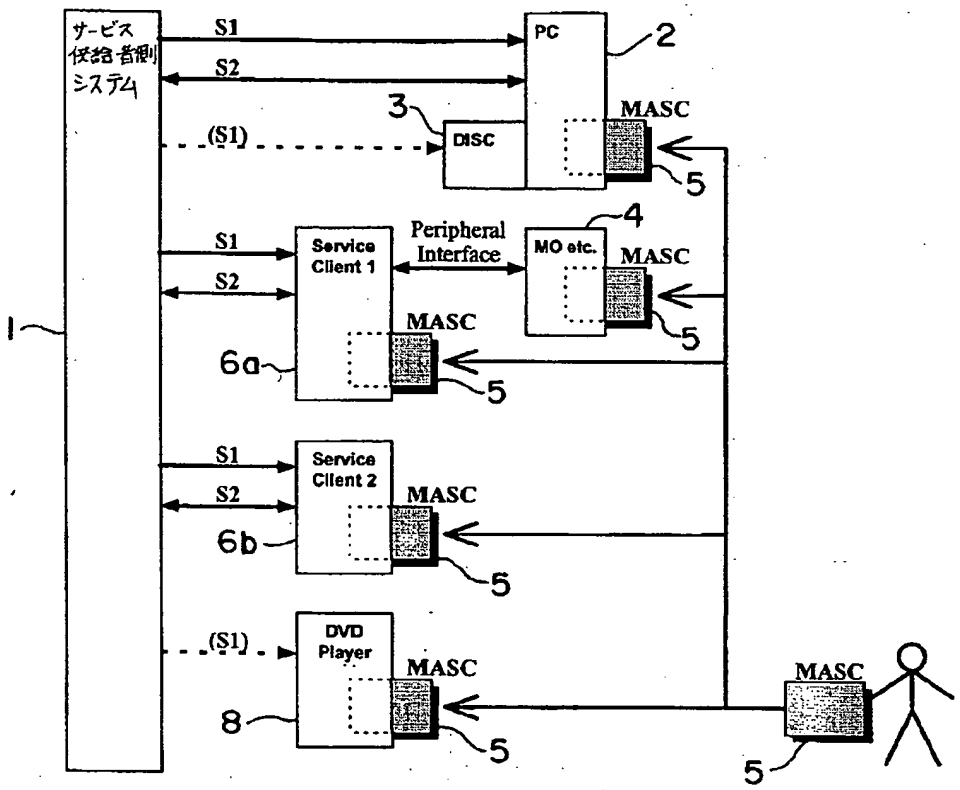
１　サービス提供者側システム
５　ＭＡＳＣ
６　サービスクライアント
１０　サーバ
１１　ユーザプロファイル
１２　第１データファイル
１３　第２データファイル
１４　デジタル署名部
１５　認証部
１６　鍵更新処理部
１８　鍵管理部
２０　乱数発生器
５３　ＤＥＳ
５５　課金情報記憶部
５７　ＲＯＭ

【図３】



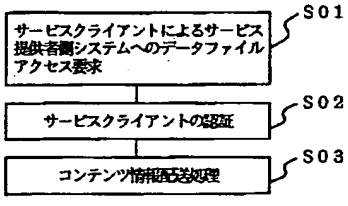
【図1】

本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図



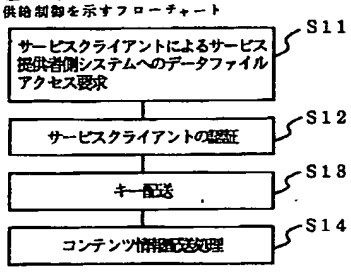
【図5】

秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート



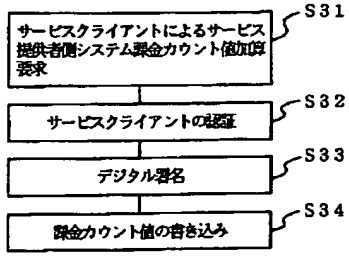
【図7】

一般のネットワークによるコンテンツ情報供給制御を示すフローチャート



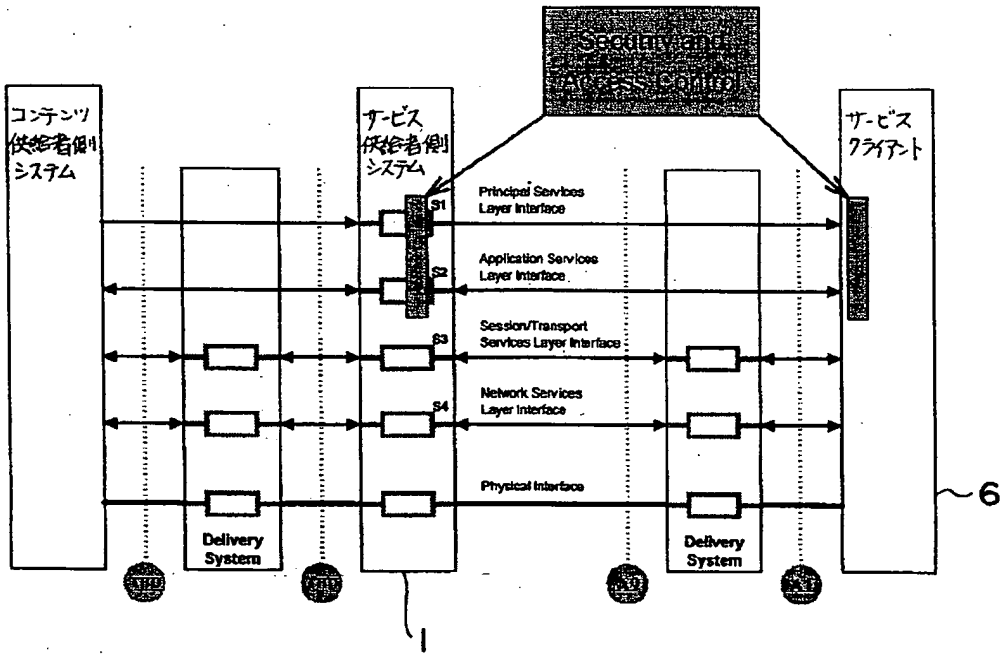
【図12】

ローカル課金処理の内容を示すフローチャート



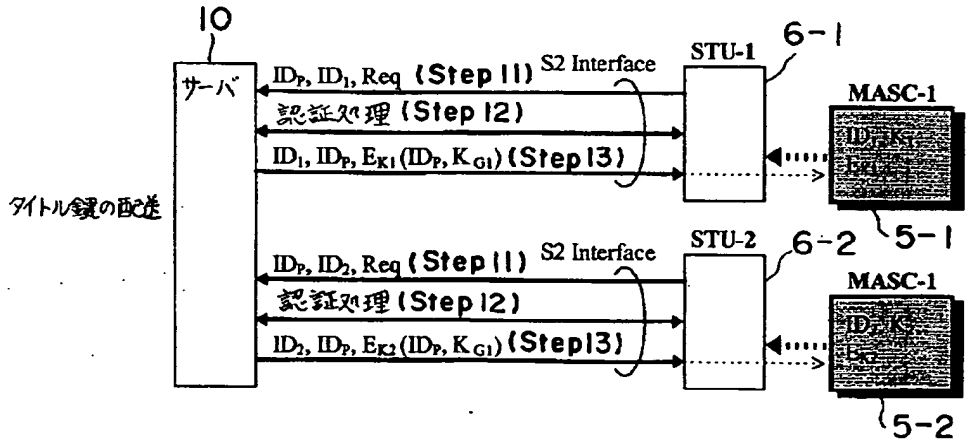
【図2】

図1のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図



【図8】

鍵配送処理を示すタイムアロー図



【図4】

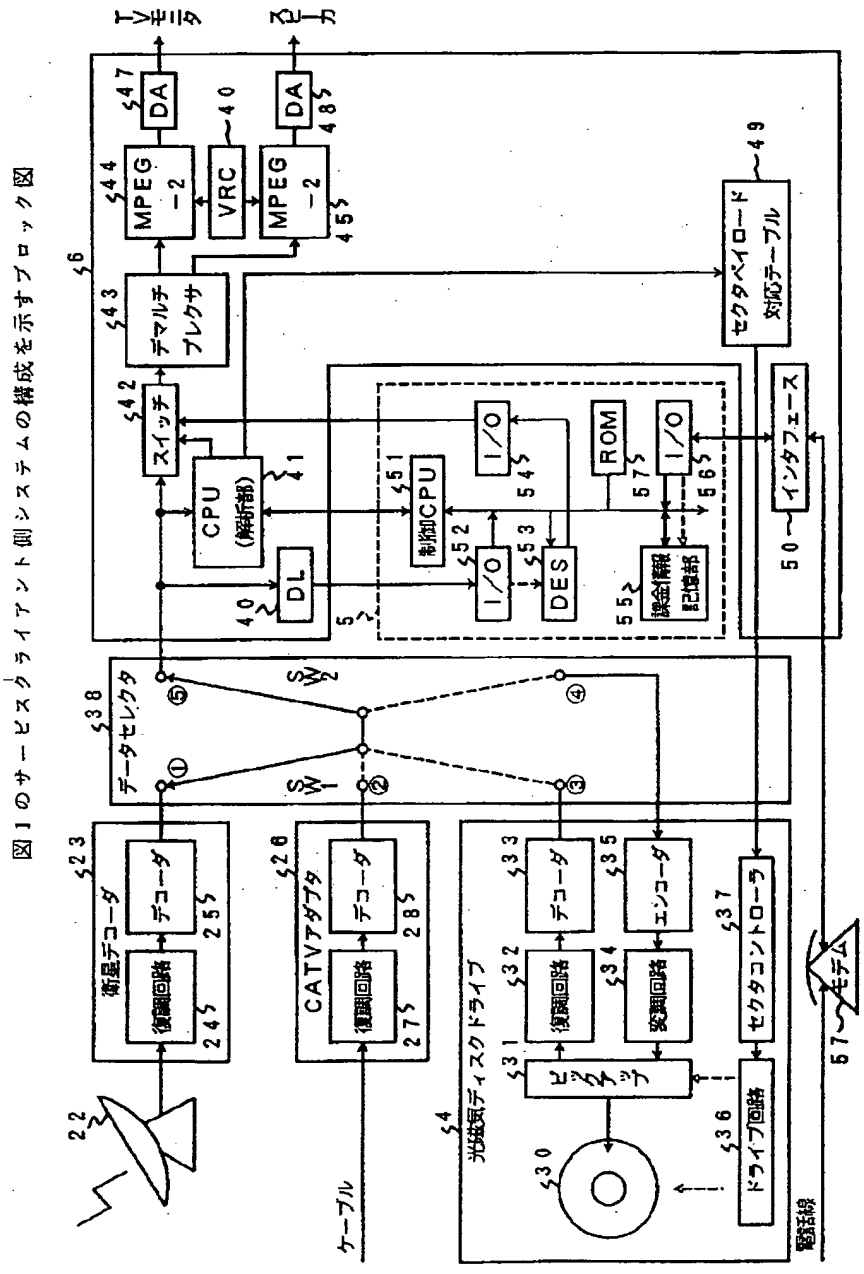
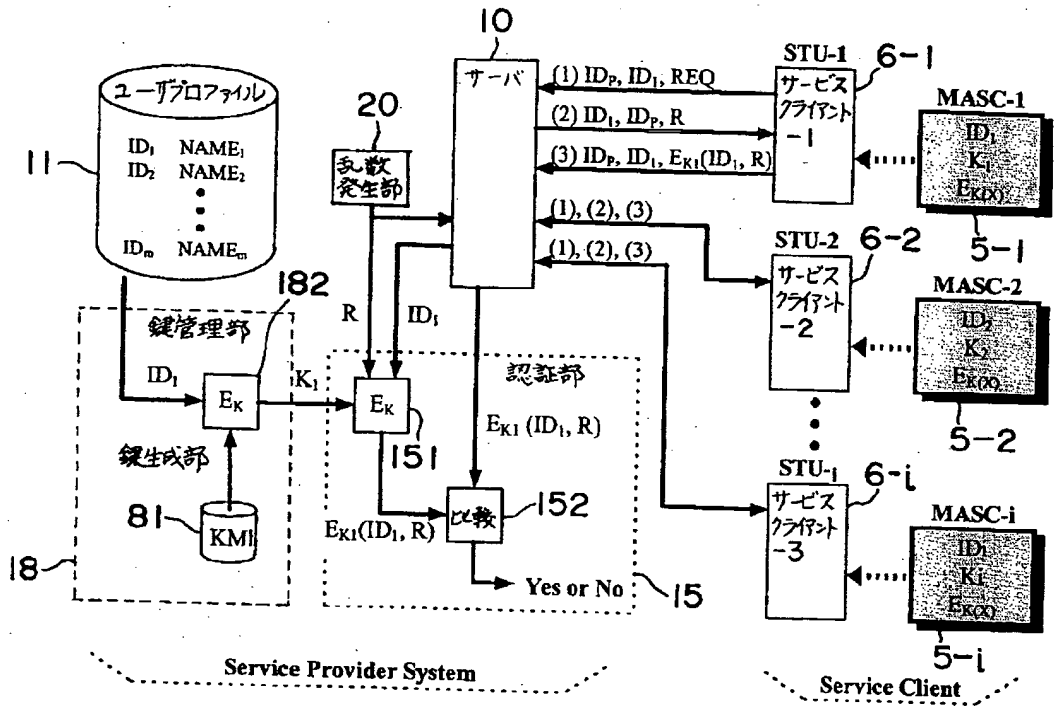


図1のサービスクライアント側システムの構成を示すブロック図
ケーブル
電話線
衛星デコーダ
CATVアダプタ
光磁気ディスクドライブ
データセレクタ
デマルチプレクサ
スイッチ
CPU（解析部）
制御CPU
DL
DES
ROM
I／O
MPEG－2
VRC
DA
デコーダ
エンコーダ
復調回路
変調回路
ピックアップ
ドライブ回路
セクタコントローラ
セクタペイロード対応テーブル
インタフェース
課金情報記憶部
モデム

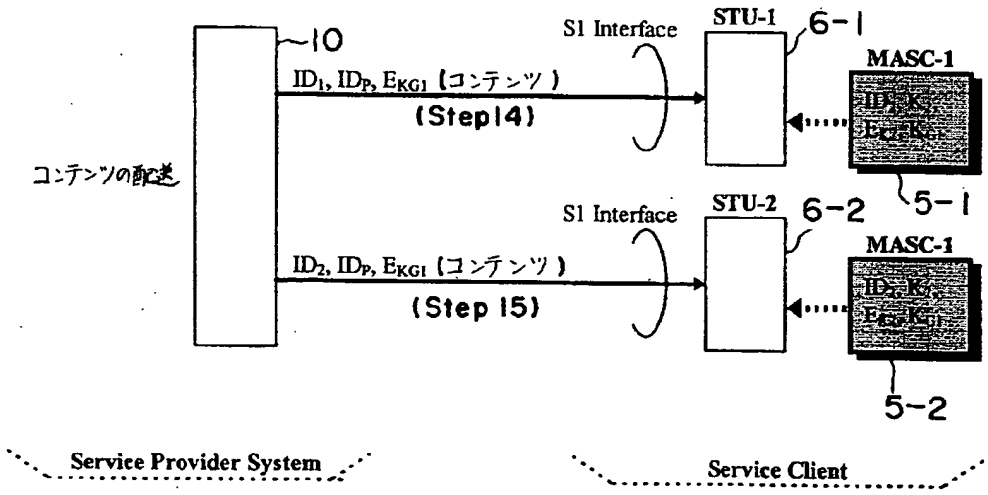
【図6】

認証処理に関連する構成を示すブロック図

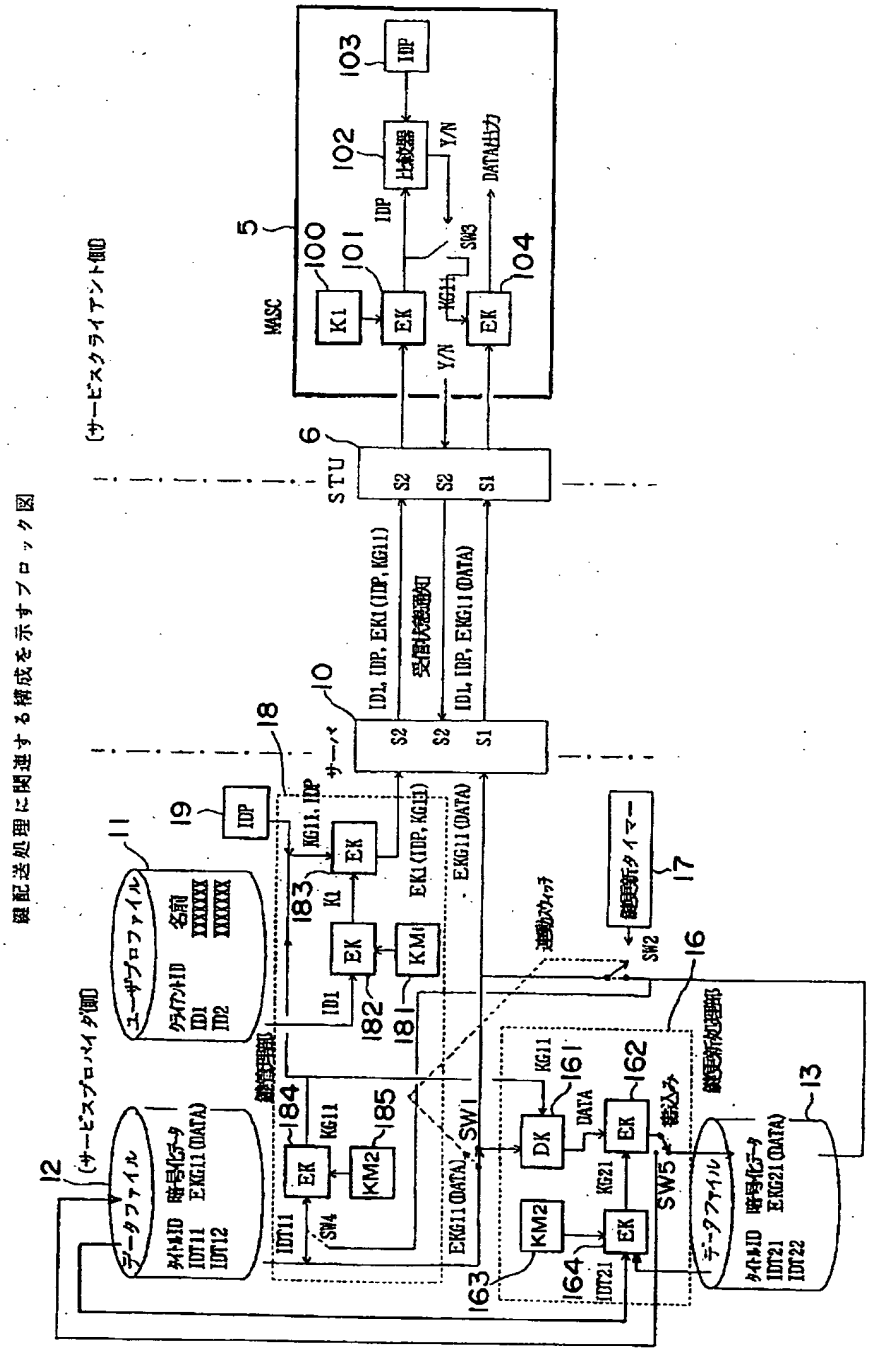


【図11】

コンテンツ配送処理を示すタイムアロー図

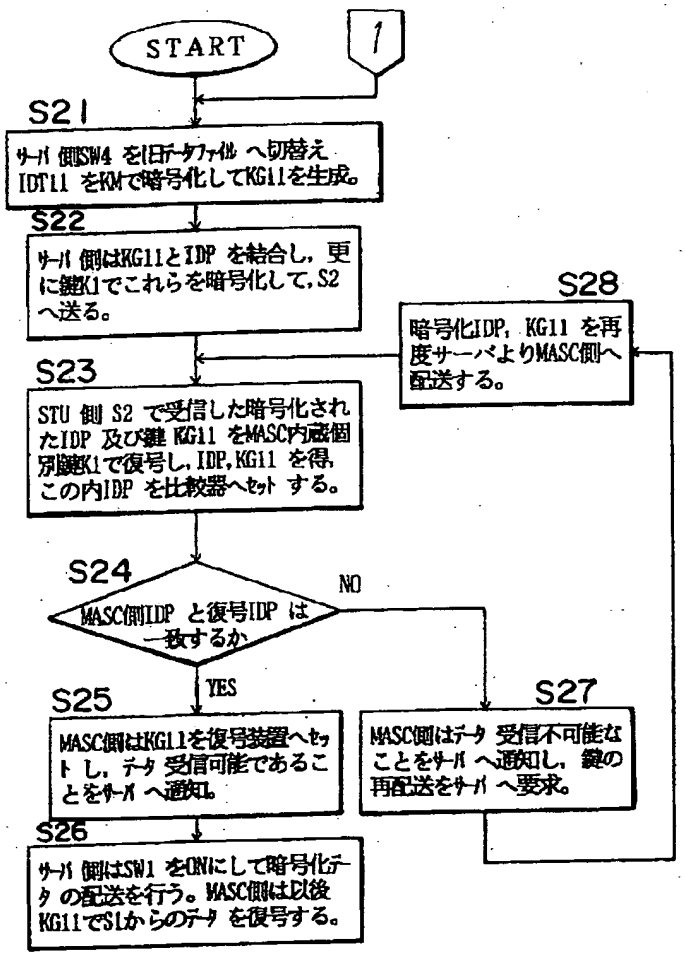


【図9】


鍵配送処理に関連する構成を示すブロック図
(サービスクライアント側)
(サービスプロバイダ側)
MASC
STU
サーバ
IDP
K1
EK
DK
KM1
KM2
KG11
KG21
SW1
SW2
SW3
SW4
SW5
Y/N
DATA出力
比較器
通信スイッチ
鍵更新タイマー
鍵更新処理部
ユーザプロファイル
データファイル
テークファイル
名前
暗号化データ
EKG11(DATA)
EKG21(DATA)
EK1(IDP, KG11)
EKG11(DATA)
IDT11
IDT12
IDT21
IDT22
ID1
ID2
S1
S2
受信状態通知
IDP, EK1(IDP, KG11)
IDP, EKG11(DATA)
DATA
書込み
10
11
12
13
16
17
18
19
100
101
102
103
104
161
162
163
164
181
182
183
184
185

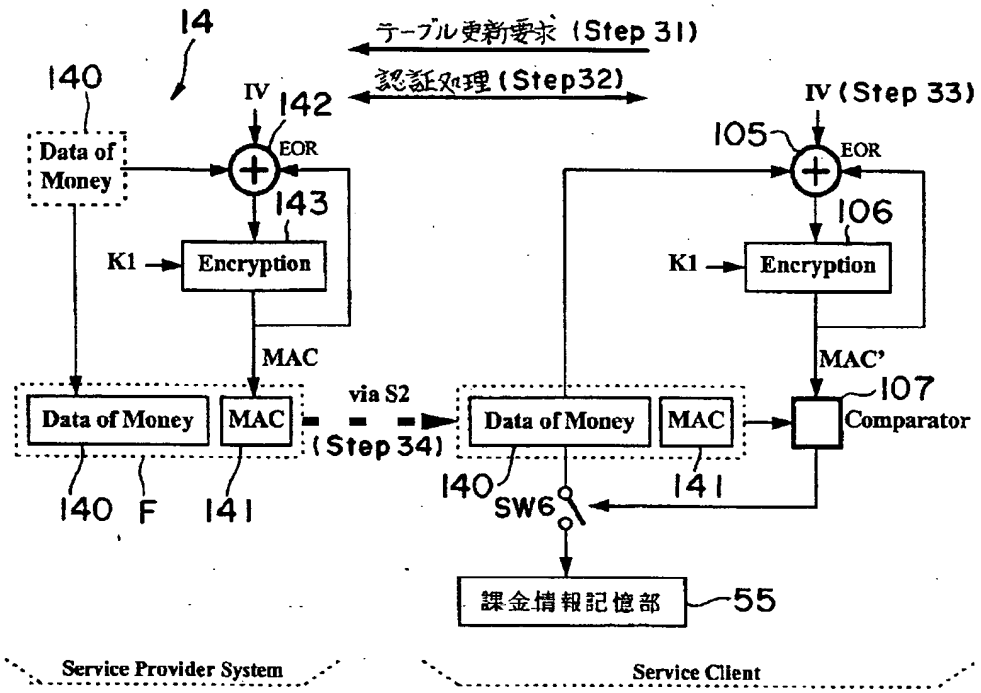
【図10】

鍵配送処理の内容を示すフローチャート



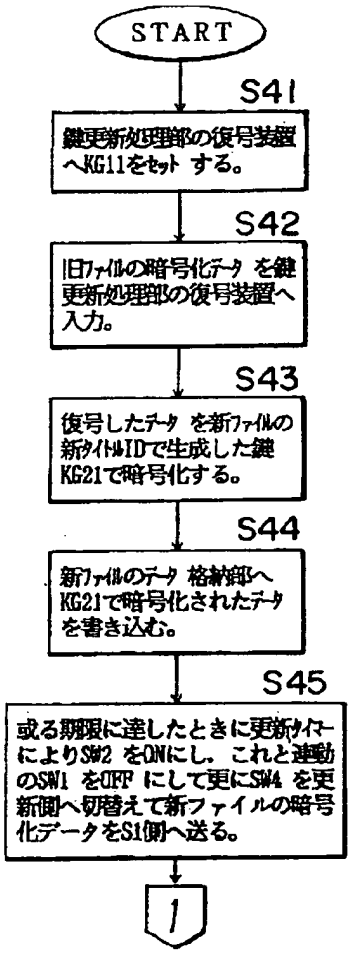
【図13】

デジタル署名処理に関連する構成を示すブロック図



【図14】

鍵の更新処理の内容を示すタイムアロー図



フロントページの続き

(72)発明者　古賀　譲
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　石崎　正之
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-215242
(43)Date of publication of application : 11.08.1998

(51)Int.Cl. H04L 9/08
G06F 15/00
G06F 17/60
G09C 1/00
H04L 9/14
// G06F 12/14

(21)Application number : 09-016085
(22)Date of filing : 30.01.1997

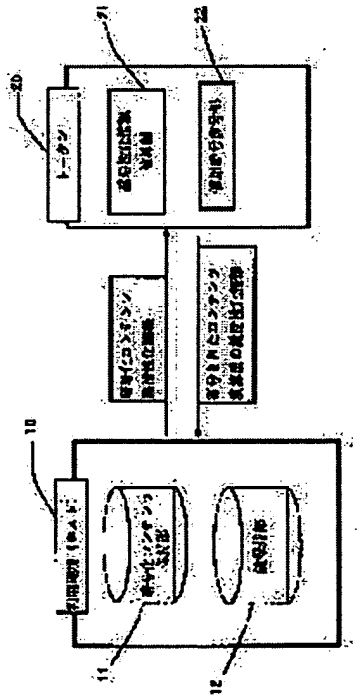
(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : KIKO KENICHIROU
SAITO KAZUO

(54) AUTHENTICATION METHOD AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To execute the control of utilization sequence of enciphered contents in off-line.

SOLUTION: In the case of using a first key, a corresponding key is retrieved from a key storage section 12 based on an ID imparted to contents. A value of a field denoting a remaining number of times corresponding to the key in the key storage section 12 and when the value is zero, a host 10 sends the contents and the key to a token 20. A decoding section 22 of the token 20 uses the key to decode the contents and sends the result to the host 10. The host 10 checks an ID of a key used next to the present key from the key storage section 12. When the ID of the next key is not zero, the host 10 retrieves the next key based on the ID and conducts key activation processing when the corresponding key is found out. When the ID of the next key is zero, since the next key is not in existence, no key activation processing is conducted. The host 10 utilizes the decoded contents.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－215242

(43)公開日　平成10年(1998)８月11日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｂ
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｚ
	17/60		Ｇ０９Ｃ	1/00	６６０Ｂ
Ｇ０９Ｃ	1/00	６６０	Ｇ０６Ｆ	12/14	３２０Ｂ
Ｈ０４Ｌ	9/14			15/21	Ｚ

審査請求　未請求　請求項の数15　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願平9－16085

(22)出願日　平成９年(1997)１月30日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　木子　健一郎
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　斉藤　和雄
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

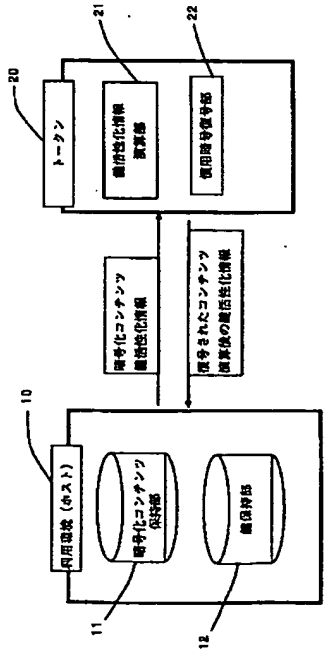
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　認証方法および装置

(57)【要約】

【課題】　暗号化されたコンテンツの利用順序の制御をオフラインで実施できるようにする。

【解決手段】　最初の鍵を使用する際にはコンテンツに付与されたＩＤを基に対応する鍵を、鍵保持部１２より検索する。鍵保持部１２の鍵に対応する残り回数のフィールドの値を調べ、値が０の場合にはホスト１０はトークン２０にコンテンツと鍵を送る。トークン２０の復号部２２は鍵を利用してコンテンツを復号しホスト１０に送る。ホスト１０は、鍵保持部１２から、現在の鍵の次に使用できる鍵のＩＤを調べる。次の鍵のＩＤが０でない場合、ＩＤをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う。次の鍵のＩＤが０の場合には、次の鍵は存在しないので、鍵活性化処理は行わない。ホスト１０は、復号されたコンテンツを利用する。



【特許請求の範囲】

【請求項１】　異なる認証を所定の順序で行う認証方法において、
先順序の認証のために対応する先順序の証明情報を利用するステップと、
上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、
上記後順序の認証のために上記後順序の証明情報を利用するステップとを有することを特徴とする認証方法。

【請求項２】　順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列を利用して上記証明情報に対応した認証を行う認証方法において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしたことを特徴とする認証方法。

【請求項３】　複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項２記載の認証方法。

【請求項４】　証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項２記載の認証方法。

【請求項５】　順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先である証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしたことを特徴とする証明情報生成方法。

【請求項６】　複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにした請求項５記載の証明情報生成方法。

【請求項７】　利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先である鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにした請求項５記載の証明情報生成方法。

【請求項８】　特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置であって、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段を有することを特徴とするユーザ認証装置。

【請求項９】　一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにすることを特徴とする暗号鍵利用順序制御方法。

【請求項１０】　複数の鍵から生成された複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成される請求項９記載の暗号鍵利用順序制御方法。

【請求項１１】　暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成される請求項９記載の暗号鍵利用順序制御方法。

【請求項１２】　一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしたことを特徴とする暗号鍵生成方法。

【請求項１３】　複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項

１２記載の暗号鍵生成方法。

【請求項１４】　利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項１２記載の暗号鍵生成方法。

【請求項１５】　暗号化されたデジタル情報を復号して利用するための復号装置であって、復号鍵によって当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段を有することを特徴とした復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の認証を所定の順序で行う認証技術に関し、その順序を逸脱した場合には認証が正しく行われないようにしたものである。また本発明は、先の順序の証明情報を利用することにより暗号化されたデジタル情報を復号して利用する場合の、暗号鍵の生成方法に関し、あらかじめ定められた順序に従ってデジタル情報を特定の回数利用することにより、次に定められた暗号鍵が生成される技術に関する。

【０００２】なお、本発明の利用範囲はコンテンツを暗号化して流通させ、その利用順序を制御するだけにはとどまらず、一般に暗号鍵（署名のための鍵、検証のための鍵など、暗号技術における鍵、一般）の利用順序の制御を可能とするものである。

【０００３】従って例えば、電車の乗車券や映画の鑑賞券のようなチケットを電子的に発行する場合に、乗車券はキセルを防ぐために予め決められた順序でしか乗車券を使えないようにしたり、あるいはある映画を見ると別の映画を安く見ることができるなどの鑑賞券の売り方を実現する際にも、電子的に発行されたチケットの利用順序の制御にも適用することが可能である。

【０００４】

【従来技術】近年のネットワークの発達により様々な情報がデジタル化され、流通するようになってきている。デジタル情報は複写が容易であり、複写されたものは劣化しないという特質があるため、金銭的な価値を持つデジタルコンテンツ（画像、動画、プログラムなど）を暗号化して流通させ、使用時にユーザの環境で復号して利用するという流通形態が開始され始めている。ＮＴＴ社のｍｉＴａＫａＴＴａ（商標）や、ＩＢＭ社のＩｎｆｏｍａｒｋｅｔ（商標）が現在実施されている代表的なサービスである。コンテンツが共通の鍵で暗号化されて配布される場合には、一旦鍵が露呈するとその鍵が流布することによってコンテンツがただで利用されてしまうという問題がある。そこで、これらのサービスではコンテンツを利用する時にのみ、オンラインで一時的に鍵を配布し、利用が終わると鍵は捨てられるように構成されている。

【０００５】しかし、この構成ではコンテンツの利用がオンラインでしかできないことになり、ユーザに対して通信コストの負担不便を強いることになる。

【０００６】一方、それに対して特公平６－９５３０２号公報のソフトウェア管理方式や、ＷａｖｅＳｙｓｔｅｍ社の開発したＷａｖｅＣｈｉｐ（商標）などの技術では、コンテンツは予め決められた暗号鍵で暗号化されて流通させ、利用者はそれを復号するための共通の鍵の封入されたＩＣカードあるいはＩＣチップを自分のＰＣに接続し、利用したいときはその装置内で復号してコンテンツを利用するというような形態により構成している。ＩＣカードなどのデバイス内では利用するごとに履歴が取られ、後でその履歴に応じて料金を徴収するというものであった。

【０００７】しかし、この方法によるとユーザの資格などに応じて、利用可能なコンテンツを制限したりすることは不可能であった。

【０００８】そこで、本出願人はあらたなユーザ認証技術を提案している（特願平９－４１８号）。この提案によれば、コンテンツは共通の鍵で暗号化し、ユーザは自分自身の鍵を持ち、アクセスチケットと呼ぶコンテンツとユーザの間を取り持つためのチケットを導入することで、暗号化されたコンテンツのオフラインでの利用を可能とし、さらにユーザ毎にアクセスチケットの発行をコントロールして、アクセス制限を行うことを可能としている。

【０００９】

【発明が解決しようとする課題】しかしながら、特願平９－４１８号の提案によると、コンテンツを利用するためのアクセスチケットはそれを発行可能であるコンテンツの配布者あるいはチケット発行センターのような機関に依頼せねばならない（以下、簡単のためこれらを総称してセンターと呼ぶ）。すなわち、ユーザはアクセスチケットを一旦手に入れてしまえばオフラインで使い続けることが可能となるが、新たなコンテンツを利用しようとした場合には前記センターにオンライン（あるいはそれに代わる手段）で依頼しなければならないことになる。

【００１０】予め幾つかの部分に分割され、それらが順序だてて利用されることを想定して作られたコンテンツ、例えば小説や物語、段階を追って難しくすることを意図した問題集などでは、これらのコンテンツは部分に分割され、それぞれの部分ごとに異なった暗号化が施さ

れ、それぞれ利用する際には異なるアクセスチケットを要求するように構成される。

【００１１】しかし、コンテンツの利用順序を限定しようとするためには、センターはユーザに対して一括してアクセスチケットを発行することはできないため、ユーザは新たな部分を利用したいと思う度にアクセスチケットを手に入れるためにセンターに発行を依頼しなければならないことになる。

【００１２】また、利用順序が線形でなく、二つの異なったコンテンツを順序に関わりなく利用することにより、別のコンテンツが利用可能になるという、提供方法もある。このような販売形態を採ろうとすると、従来の方法では、やはりユーザは三つ目のコンテンツを利用するためのチケットをセンターに発行依頼しなければならない。

【００１３】

【発明が解決しようとする課題】本発明は上記のような問題に鑑みてなされたものであり、その目的とするところは、ユーザによる暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御をオフラインで実施可能であるようにすることにある。

【００１４】

【課題を解決するための手段】まず、本発明の概要について具体的な実現環境に即して説明する。本発明の１実現環境では、上記の課題を解決するため、ユーザ環境をコンテンツの利用環境と、あらかじめユーザ毎に配られるトークンによって構成する。トークンはＩＣカードなどの演算機能を持つ耐タンパー容器である。そして、ある鍵に対して特定の演算を複数回繰り返す事で、始めて次に指定された鍵が生成されるように計算された複数の鍵を発行し、ユーザ環境においてトークンがこの定められた演算を行った結果を基にして、次の鍵を生成することで次の鍵が利用可能になる。

【００１５】また、本発明は上記の課題を解決するため、アクセスチケットを用いたアクセス制御方法（特願平９－４１８号）において、一連の複数のチケットとそれぞれのチケットに対応する利用制限情報をあらかじめ決められた計算方法に基づいて発行する。アクセスチケットの利用制限情報には、このチケットの使用順位もしくは次に使用するチケットを識別する数値、次のチケットを使用可能にするためのチケット活性化情報、次のチケットが使用可能になるまでの回数、及び次のチケットの法数のフィールドが含まれる。そして、発行した複数のチケットと、最初に用いるチケットに対応する利用制限情報のみをユーザに配布する。

【００１６】あるチケットの次のチケットを使用可能にするためのチケット活性化情報は、現在使用しているチケットを用いて、トークンとの間で定められた回数の通信を行う事でのみ生成される。こうして生成されたチケット活性化情報を、次に使用するチケットの利用制限情報の特定のフィールドに追加する事により、はじめて次のチケットが使用可能になる。

【００１７】次のチケットは異なるコンテンツに対するものであってもよいし、同一のコンテンツに対して、異なる利用条件での使用を許可するものであってもよい。

【００１８】さらに、本発明の構成について詳細に説明する。

【００１９】本発明によれば、上述の目的を達成するために、異なる認証を所定の順序で行う認証方法において、先順序の認証のために対応する先順序の証明情報を利用するステップと、上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、上記後順序の認証のために上記後順序の証明情報を利用するステップとを実行するようにしている。

【００２０】この構成においては、先順序の証明情報を実際に使用して初めて後順序の証明情報が利用可能になり、認証を所定の順番で行うように強制できる。

【００２１】また、本発明によれば、上述の目的を達成するために、順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列の利用して上記証明情報に対応した認証を行う認証法補において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしている。

【００２２】この構成においては、先の証明情報が利用されて、後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【００２３】また、この構成において、複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【００２４】また、証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【００２５】また、本発明によれば、上述の目的を達成するために、順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先であ

る証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしている。

【００２６】この構成においても、先の証明情報が利用されて、後の証明情報が生成されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【００２７】また、この構成において、複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【００２８】また、利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先である鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【００２９】また、本発明によれば、上述の目的を達成するために、特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置でおいて、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段とを設けるようにしている。

【００３０】この構成においても、先の証明情報が利用されて後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【００３１】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにしている。

【００３２】この構成においては、複数の鍵から生成された複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成されるようにしてもよい。

【００３３】また、暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成されるようにしてもよい。

【００３４】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしている。

【００３５】この構成においては、複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよいまた、利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよい。

【００３６】また、本発明によれば、上述の目的を達成するために、暗号化されたデジタル情報を復号して利用するための復号装置に、復号鍵によって、当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段とを設けるようにしている。

【００３７】この構成においては、先行する復号鍵を利用することにより後続の復号鍵を活性化させることで可能となり、予め定められた順序で復号を行うことが可能となる。

【００３８】

【発明の実施の態様】以下、本発明の実施例について説明する。

【００３９】［実施例１］本実施例では、１つの暗号化

鍵を特定の回数用いる事により、異なるコンテンツに対する暗号化鍵を生成する方法について述べる。

【００４０】本実施例は、デジタルコンテンツを暗号化して鍵と共に提供するコンテンツプロバイダと、提供されたコンテンツを復号して利用するためのユーザ環境とからなる。

【００４１】図１は、ユーザ環境を示しており、この図において、ユーザ環境は、利用環境（ホスト）１０とトークン２０とからなり、利用環境１０は暗号化されたデジタルコンテンツを保持するコンテンツ保持部１１と、それに対応する鍵を保持する鍵保持部１２とを含んで構成されている。トークン２０はあらかじめユーザ毎に配布される、スマートカードやＩＣカードであり、鍵を活性化させるための演算部２１とコンテンツ、もしくはコンテンツを復号するための情報を復号するための復号部２２を持つ。

【００４２】次に実施例の動作について図２および図３を参照して述べる。図２は実施例の全体的な処理を示す。図３は鍵活性化処理の詳細を示す。

【００４３】なお、本実施例では、コンテンツプロバイダは４つの異なるコンテンツが順番に利用されるように、鍵を発行する。始めにコンテンツプロバイダは、コンテンツを慣用暗号鍵Ｋ１で暗号化する。さらに、他のコンテンツを、利用する順番にそれぞれＫ２～Ｋ４の鍵で暗号化する。そして、以下のように、Ｋ２′～Ｋ４′を計算する。

【００４４】

【数１】$K2' = K2 - F^{Ur2}(K1)$

$K3' = K3 - F^{Ur3}(K2)$

$K4' = K4 - F^{Ur4}(K3)$

$F^{Ur2}(K1)$はＫ１に対してＦの演算をＵｒ２回繰り返す事を意味している。

【００４５】Ｆは一方向性関数（例えばＭＤ５などのハッシュ関数）、Ｕｒは次のチケットを使用可能にするために現在のチケットを使用しなければならない回数である。Ｆの計算方法を秘密とし、ユーザ毎にその計算方法を異なるものとすれば、他のユーザが計算した値を流用される事はない。ユーザには、Ｋ１とＫ２′～Ｋ４′および、Ｕｒ２～Ｕｒ４が配布される。ユーザに配布された鍵は鍵保持部１２に保持される。一連の鍵が配布された時点での、鍵保持部１２の様子を図４に示す。

【００４６】さて、図２において、最初の鍵を使用する際にはコンテンツに付与されたＩＤを基に対応する鍵を、鍵保持部１２より検索する（Ｓ１０）。対応する鍵が無い場合は処理を終了する（Ｓ１１）。次に、鍵保持部１２の鍵に対応する残り回数のフィールドの値を調べ、値が０でない場合はその鍵はまだ有効ではないので、やはり処理を終了する（Ｓ１２）。ホスト１０はトークン２０にコンテンツと鍵を送る（Ｓ１３）。トークン２０の復号部２２は鍵を利用してコンテンツを復号しホスト１０に送る（Ｓ１４）。ホスト１０は、鍵保持部１２から、現在の鍵の次に使用できる鍵のＩＤを調べる（Ｓ１５）。次の鍵のＩＤが０でない場合、ＩＤをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う（Ｓ１６～Ｓ１９）。次の鍵のＩＤが０の場合には、次の鍵は存在しないので、ホスト１０は復号されたコンテンツを利用する（Ｓ２０）。

【００４７】次に図３を参照して鍵活性化処理Ｓ１９について詳細に述べる。図３において、鍵活性化処理では、まず鍵保持部１２から鍵に対応する鍵活性化情報を取得する（Ｓ２１）。この値が０であった場合には、鍵活性化情報のフィールドに、現在の鍵の値を書き込む（Ｓ２２、Ｓ２３）。次に、ホスト１０はトークン２０に現在の鍵活性化情報αを送る（Ｓ２４）。トークン２０はＦ（α）を計算しホスト１０にその値を返す（Ｓ２５）。鍵保持部１２の、次の鍵の残り回数Ｕｒの値（図４）を１減らす（Ｓ２６）。１減らした結果、残り回数Ｕｒの値が０にならない場合には、ユーザ環境はＦ（α）の値で、現在の鍵の活性化情報を置き換える（Ｓ２７、Ｓ２８）。値が０になった場合には、次の鍵の値にＦ（α）を足したもので、次の鍵の値を置き換える（Ｓ２９）。このようにして２番目の鍵が使用可能になった時点での、鍵保持部の様子を図５に示す。これで、鍵活性化処理は終了し、ホスト１０は復号されたコンテンツを利用する。

【００４８】このように一連の鍵を上記のような方法で、関連付けて作成する事により、第一の鍵Ｋ１を特定回数使うことにより、初めて、第二の鍵Ｋ２を計算する事ができ、これにより第二の鍵Ｋ２が利用可能になる。同様の処理により、順次異なる鍵を、定まった順序・回数でのみ利用する仕組みが実現できる。

【００４９】［実施例２］本実施例では、特に１つのコンテンツを特定の回数用いる事により、異なる利用条件での使用を可能にする方法について述べる。例えば、あるコンテンツを特定回数用いることで、より安い料金での使用を可能にするような方法である。

【００５０】また、本実施例は、本発明を特願平９－４１８号のユーザ認証技術に適用した例である。

【００５１】はじめに、本実施例で用いられるアクセスチケット（認証用補助情報）を用いた処理の概観を説明する。図６に処理の概観を示す。図６において、アクセスチケットを用いた処理は、チケット発行センタ３０と、コンテンツプロバイダ４０、及びユーザ環境５０から構成されるシステムにおいて実行される。

【００５２】チケット発行センタ３０は、チケット公開鍵データベース３１、ユーザデータベース３２、プロバイダデータベース３３及びアクセスチケット発行装置３４を持つ。コンテンツプロバイダ４０は、暗号化していないコンテンツと、慣用暗号鍵を保持し、慣用暗号装置よりコンテンツを暗号化する。

【００５３】また、ユーザ環境５０は、パソコンやワークステーションなど、ディジタル情報を利用するための情報処理装置である利用環境（ホスト）５１と、利用者の認証をするためにホスト５１に接続されているトークン５２とを含んでなる。ホスト５１はユーザツール５３およびカプセル化コンテンツ５４を含む。トークン５２は、各利用者に固有の情報を安全に封入したＩＣカードもしくはスマートカードのような耐タンパー容器であり、固有情報をもとに利用者の認証を行うための演算部を有している。トークン５２はあらかじめ各利用者に配布されている。

【００５４】はじめに、コンテンツプロバイダ４０は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｌｅｍａｎ）公開鍵の発行を、チケット発行センタ３０に対して要求する（①）。チケット発行センタ３０は要求に応じて、公開鍵をコンテンツプロバイダ４０に送付する（②）。コンテンツプロバイダ４０は自身で用意した慣用暗号鍵でコンテンツを暗号化し、その鍵をさらに発行された公開鍵で暗号化してコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（カプセル化コンテンツ）が、利用者（ユーザ環境）５０にネットワークやＣＤ－ＲＯＭなどを用いて配布される（③）。コンテンツは暗号化されているため、このままでは利用する事ができない。利用者は利用したいコンテンツ及び自分のユーザＩＤに対応したアクセスチケットの発行をセンタ３０に要求する（④）。アクセスチケットは、特定のコンテンツとユーザの固有情報がそろったときにのみ、そのコンテンツを利用可能にするためのディジタル情報であり、他のユーザとコンテンツの組み合わせでは使用できない。センタ３０はユーザの要求に応じてアクセスチケットを発行しユーザに送付する（⑤）。ユーザはアクセスチケットを用いてコンテンツを利用する。アクセスチケットにはアクセス制御のための情報以外に、利用料金や支払方法、使用期限などの利用条件に関する情報が付与されている。ユーザがコンテンツを利用すると、利用に応じてその履歴がトークン５２に記録される。この際、履歴にはその利用時点での利用条件も同時に記録される。ユーザは適当なタイミングで、センタ３０に利用履歴を送付する（⑥）。センタ３０は回収した利用履歴に基づいて課金を行う。回収した履歴に基づいて計算された料金が、それぞれの利用者の口座より引き落とされ、コンテンツプロバイダ４０に各コンテンツの利用量に応じて分配される（⑦）。

【００５５】次に、本実施例での処理を詳しく説明する。

【００５６】はじめに、コンテンツプロバイダ４０は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なＲＳＡ公開鍵ペアＥ，Ｄと法数ｎをセンタ３０より発行してもらう。コンテンツプロバイダ４０にはＥとｎが渡され、センタ３０は発行した公開鍵に対応する秘密鍵Ｄ、法数ｎを公開鍵データベース３１に記録して安全に管理しておく。次に、コンテンツプロバイダ３０は自身で用意した慣用暗号鍵Ｋによりこのコンテンツを暗号化する。さらに、このＫをセンタより発行された公開鍵Ｅで暗号化し、$K^* = K^E \bmod n$を作成する。このK^*をコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（以下カプセル化コンテンツと呼ぶ）は、利用者にネットワークやＣＤ－ＲＯＭなどを用いて配布される。

【００５７】ユーザはコンテンツを利用するため、アクセスチケットの発行をセンタ３０に依頼する。図７にアクセスチケットの構成を示す。アクセスチケットは認証用情報（以下単にチケットと呼ぶ）ｔと、利用制限情報Ｌ、チケット法数ｎ、及び公開鍵Ｅからなる。アクセスチケットとコンテンツは一意に対応しており、コンテンツの公開鍵法数ｎによって対応関係を決定することができる。

【００５８】ここで、ある一定回数の利用後には異なった利用条件（例えば割引料金）での使用を可能にするため、アクセスチケットを発行する際に、センタ３０は以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では４種類の異なる利用条件を持つアクセスチケットとそれに対応する利用制限情報を用意する。

【００５９】

【数２】ｔ１＝Ｄ＋Ｆ（ｄｕ，Ｌ１，ｎ）
ｔ２＝Ｄ＋Ｆ（ｄｕ，Ｌ２，ｎ）
ｔ３＝Ｄ＋Ｆ（ｄｕ，Ｌ３，ｎ）
ｔ４＝Ｄ＋Ｆ（ｄｕ，Ｌ４，ｎ）

利用制限情報を図８に示す。

【００６０】上記の式および図８において、式「$(\alpha 1)^{FUr2(du,L1,n)} \bmod n$」は、$\alpha 1$をＦ（ｄｕ，Ｌ１，ｎ）でＵｒ２回べき乗し、ｎに関する剰余をとることを表す。ｔはチケット、Ｄはコンテンツの公開鍵に対応する秘密鍵、Ｆは一方向性関数（例えばＭＤ５などのハッシュ関数）、ｄｕはユーザの秘密鍵、ｎはコンテンツの公開鍵法数、Ｉｒはチケット発行時に生成される乱数、Ｌは利用条件などを記した利用制限情報である。

【００６１】利用制限情報Ｌは、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の１回の利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報Ｌには、このアクセスチケットの使用順位、次のアクセスチケットを使用可能にするためのチケット活性化情報α、及び次のアクセスチケットが使用可能になるまでの回数Ｕｒが含まれている。

【００６２】チケット生成時には、ｔはＬを図８に示すように設定して計算される。すなわち、Ｕｒの値を全て０とし、αの計算にのみ実際のＵｒの値が用いられる。ｎ、Ｄの値はセンタ３０内の公開鍵データベース３１を、ｄｕの値はユーザデータベース３２を参照する事により得ることができる。

【００６３】ユーザにはｔ１からｔ４の一連のチケットと、利用制限情報Ｌ１～Ｌ４を含むアクセスチケットが配布される。但し、ユーザへの配布時にはＬ１～Ｌ４は、図９に示すようにＵｒ１～Ｕｒ４に値が設定され、さらにＬ２～Ｌ４のα２～α４の値を０としたものに置き換えられる。

【００６４】図１０にユーザ環境５０（図６）の構成を示す。ユーザ環境５０は利用環境（ホスト）５１とトークン５２からなり、トークン５２は証明情報演算部６４およびユーザ固有情報保持部６５を有している。ユーザ固有情報保持部６５には各ユーザに固有の情報が入れられている。固有情報はユーザには秘密であり、ユーザのＩＤとそれに対応する固有情報は、チケット発行センタ３０で安全に管理されている。

【００６５】利用環境（ホスト）５１は、カプセル化コンテンツ５４とユーザツール５３とを有する。ユーザツール５３は、アクセスチケット保持部（複数のチケット）５５、アクセスチケット検索部５６、および証明情報演算部５７を持つ。また、カプセル化コンテンツ５４には、乱数発生部５８、チケット公開鍵法数保持部５９、チケット公開鍵保持部６０、慣用暗号復号部６１、暗号化された慣用鍵の保持部６２、および暗号化コンテンツ保持部６３を有する。

【００６６】次に、ユーザ環境５０での処理について述べる。図１１および図１２にユーザ環境５０での処理を示す。ユーザ環境では以下の処理を行う。

［ステップＳ３１］　カプセル化コンテンツ５４が乱数ｒを生成する。

［ステップＳ３２］　カプセル化コンテンツ５４が$r^E K^E \bmod n$を計算し、この値とコンテンツの公開鍵法数ｎとをユーザツール５３に送付する。ｒを用いるのはトークンとの通信路上で慣用暗号鍵を知られるのを防ぐためである。

［ステップＳ３３］　ユーザツール５３が、管理しているチケット保持部５５から、ｎを法数として持つアクセスチケットを全て検索する。チケット保持部５５は、法数ｎと対応するチケットを組にして保持している。

［ステップＳ３４］　アクセスチケットが１つも見つからない場合は、処理を終了する。

［ステップＳ３５］　検索したチケットの中から、利用制限情報の残り使用回数Ｕｒが０のチケットで、最も使用順位の値が大きいものを選択する。

［ステップＳ３６］　現在のチケットと同じ法数ｎを持つチケットの中から、現在のチケットの次に使用順位の値が大きいチケットを検索する。

［ステップＳ３７、Ｓ３８、Ｓ３９］　チケットが見つかった場合、そのチケットの活性化情報の値を調べ、その値が０の場合には現在のチケットの活性化情報の値を書き込む。そして、$r^E K^E \bmod n$，法数ｎ，現在のチケットの利用制限情報Ｌ、及び次のチケットの活性化情報αの値をトークン５２に送る。活性化情報がゼロでない場合はそのまま$r^E K^E \bmod n$，法数ｎ，現在のチケットの利用制限情報Ｌ、及び次のチケットの活性化情報αの値をトークン５２に送る。

［ステップＳ３６、Ｓ４０］　チケットが見つからない場合、αの値を０をとして、$r^E K^E \bmod n$，ｎ，Ｌ、αの組みをトークン５２に送る。

［ステップＳ４１］　トークン５２が、

【００６７】

【数３】$R1 = (r^E K^E)^{F(du,L,n)}$

$R2 = (\alpha)^{F(du,L,n)}$

を計算する。

［ステップＳ４２］　ユーザツール５３は、トークン５２が計算を行っている間に、$(r^E K^E)^t$の値を計算する。

［ステップＳ４３］　トークン５２は、計算したＲ１、Ｒ２の値をユーザツール５３に送る。

［ステップＳ４４～Ｓ４６］　次の使用順位のチケットがある場合には、ユーザツール５３は次のチケットの利用制限情報中の残り回数Ｕｒの値を１減らし、さらに、次のチケットの活性化情報フィールドの値を、Ｒ２の値で置き換える。

［ステップＳ４７］　トークン５２から受け取ったＲ１から、

$(r^E K^E)^t \cdot R1^{-1} = r^K \bmod n$

を計算してカプセル化コンテンツ５４に送付。

［ステップＳ４８］　カプセル化コンテンツ５４は、ｒＫよりＫを求める。ｒの値はカプセル化コンテンツ４９が発生させたものなので、Ｋの計算が可能である。

［ステップＳ４９］　カプセル化コンテンツ５４は、Ｋにより暗号化されたコンテンツ本体を慣用暗号復号部６１により復号して利用する。

【００６８】最初のチケットｔ１を１回使用した時点での、利用制限情報は図１３に示すようになる。

【００６９】ユーザがコンテンツを利用すると、その利用時点での利用条件がトークン５２に履歴として記録される。同じコンテンツであっても利用時点での利用条件での履歴が記録されるため、定まった利用順序・回数で定まった利用条件によるコンテンツの利用が可能になる。

【００７０】このようにチケットと利用制限情報の組を計算しておくことにより、例えば、第一のチケットｔ１を特定回数使うことで始めて、ｔ２の計算に用いられたＬ２中のα２を計算する事ができ、第二のチケットが利

用可能になる。第２のチケットの利用条件を第１のチケットと異なるものとすることで、例えば利用料金の割引などを行う事が可能になる。同様の処理により、順次異なった条件のチケットを、定まった順序・回数で利用する仕組みが実現できる。

【００７１】［実施例３］本実施例では特に、１つのコンテンツを特定の回数用いる事により、それとは異なったコンテンツの使用を定められた順番で可能にする方法について述べる。

【００７２】本実施例では実施例２と同様にアクセスチケットによる処理を行う。

【００７３】本実施例の構成は実施例２と同様であるが、アクセスチケットの利用制限情報に、使用順位の代わりに、次に使用可能となるコンテンツに対応する法数を入れるフィールドが追加される点が異なる。

【００７４】実施例の動作について説明する。

【００７５】実施例２と同様の方法により、コンテンツプロバイダ４０はセンタ３０から発行してもらった公開鍵を用いてコンテンツをカプセル化して配布する。ユーザは同様に、センタ３０に対してアクセスチケットの発行を要求する。

【００７６】ここで、あるコンテンツを特定回数利用した場合のみ、それとは異なるコンテンツを定まった順番で利用できるようにするため、アクセスチケットを発行する際に、センタは以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では４種類の異なったコンテンツと、それぞれのコンテンツに対応するアクセスチケットとそれに対応する利用制限情報（図１４）を用意する。

【００７７】アクセスチケットは次式のようなものである。

【００７８】

【数４】ｔ１＝Ｄ１＋Ｆ（ｄｕ，Ｌ１，ｎ１）
ｔ２＝Ｄ２＋Ｆ（ｄｕ，Ｌ２，ｎ２）
ｔ３＝Ｄ３＋Ｆ（ｄｕ，Ｌ３，ｎ３）
ｔ４＝Ｄ４＋Ｆ（ｄｕ，Ｌ４，ｎ４）

利用制限情報は図１４に示すようなものである。

【００７９】上記の式および図１４において式「（α１）$^{FUr2(du,L1,n2)}$　ｍｏｄ　ｎ」は、α１をＦ（ｄｕ，Ｌ１，ｎ２）でＵｒ２回べき乗し、ｎに関する剰余をとることを表す。ｔはチケット、Ｄはコンテンツの公開鍵に対応する秘密鍵、Ｆは一方向性関数（例えばＭＤ５などのハッシュ関数）、ｄｕはユーザの秘密鍵、ｎはコンテンツの公開鍵法数、Ｉｒはチケット発行時に生成される乱数、Ｌは利用条件などを記した利用制限情報である。

【００８０】利用制限情報Ｌは、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の１回の利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報Ｌには、次のアクセスチケットを使用可能にするためのチケット活性化情報α、次のアクセスチケットが使用可能になるまでの回数Ｕｒ、および次に使用可能になるチケットの法数が含まれている。

【００８１】チケット生成時には、ｔはＬを上記の表のように設定して計算される。すなわち、Ｕｒの値を全て０とし、αの計算にのみ実際のＵｒの値が用いられる。

【００８２】ユーザにはｔ１からｔ４の一連のチケットと、利用制限情報Ｌ１～Ｌ４を含むアクセスチケットが配布される。但し、ユーザへの配布時にはＬ１～Ｌ４は、図１５に示すようにＵｒ１～Ｕｒ４に値が設定され、さらにＬ２～Ｌ４のα２～α４の値を０としたものに置き換えられる。

【００８３】次に、ユーザ環境での処理について述べる。ユーザ環境５０の構成は実施例２と同様である。図１６および図１７にユーザ環境５０での処理を示す。ユーザ環境５０では以下の処理を行う。

［ステップＳ５１］　カプセル化コンテンツ５４が乱数ｒを生成する。

［ステップＳ５２］　カプセル化コンテンツ５４は$r^E K^E$　ｍｏｄ　ｎを計算し、この値とコンテンツの公開鍵法数ｎをユーザツール５３に送付する。ｒを用いるのはトークン５２との通信路上で慣用暗号鍵を知られるのを防ぐためである。

［ステップＳ５３］　ユーザツール５３は、管理しているチケット保持部５５から、ｎを法数として持つチケットを検索する。チケット保持部５５は、法数ｎと対応するチケットを組にして保持している。

［ステップＳ５４］　チケットが見つからなかった場合は処理を終了する。

［ステップＳ５５］　検索したチケットの残り利用回数Ｕｒが０でなければ、そのチケットはまだ有効ではないので、処理を終了する。

［ステップＳ５６］　ユーザツール５３は現在のチケットの利用制限情報Ｌの、次のチケットの法数の値を調べる。

［ステップＳ５７～Ｓ６０］　法数の値が０ではなく、この法数に対応する次のチケットが存在する場合、そのチケットの活性化情報の値を調べ、その値が０の場合には現在のチケットの活性化情報の値を書き込む。

［ステップＳ６１］　さらに$r^E K^E$　ｍｏｄ　ｎ，法数ｎ，現在のチケットの利用制限情報Ｌ、及び次のチケットの活性化情報αの値をトークン５２に送る。

［ステップＳ６２］　次のチケットの法数の値が０か、法数の示すチケットが存在しない場合には、、αの値を０をとして、$r^E K^E$　ｍｏｄ　ｎ，ｎ，Ｌ，αの組みをトークン５２に送る。

［ステップＳ６３］　トークン５２は

【００８４】
【数５】Ｒ１＝（ｒ^{E}Ｋ^{E}）$^{F(du,L,n)}$、
Ｒ２＝（α）$^{F(du,L,n)}$
を計算する。
［ステップＳ６４］　ユーザツール５３はトークン５２が計算を行っている間に、（ｒ^{E}Ｋ^{E}）ｔの値を計算する。
［ステップＳ６５］　トークン５２は、計算したＲ１、Ｒ２の値をユーザツール５３に送る。
［ステップＳ６６～Ｓ６８］　次のチケットがある場合には、ユーザツール５３は、次のチケットの利用制限情報中の残り回数Ｕｒの値を１減らし、さらに、次のチケットの活性化情報フィールドの値を、Ｒ２の値で置き換える。
［ステップＳ６９］　トークン５２から受け取ったＲ１から、
【００８５】
【数６】（ｒ^{E}Ｋ^{E}）ｔ・Ｒ１$^{-1}$＝ｒＫ　ｍｏｄ　ｎ
を計算してカプセル化コンテンツ５４に送付する。
［ステップＳ７０］　カプセル化コンテンツ５４は、ｒよりＫを求める。ｒの値はカプセル化コンテンツ５４が発生させたものなので、Ｋの計算が可能である。
［ステップＳ７１］　カプセル化コンテンツ５４は、Ｋにより暗号化されたコンテンツ本体を慣用暗号復号部６１により復号して利用する。
【００８６】最初のチケットｔ１を１回使用した時点での、利用制限情報は図１８に示すようになる。
【００８７】実施例２と同様の方法により、ユーザの利用に応じて利用履歴がトークン５２に記録され、これをセンタ３０が回収する事により、利用者への課金とコンテンツプロバイダ４０への料金の分配が行われる。
【００８８】このようにチケットと利用制限情報の組をあらかじめ計算して配布することにより、例えば、第一のチケットｔ１を特定回数使うことで始めて、ｔ２の計算に用いられたＬ２中のα２を計算する事ができ、第二のチケットが利用可能になる。第２のチケットには異なるコンテンツが対応づけられており、これにより、定まった順序で次のコンテンツを使用させる事ができる。同様の処理により、順次異なったコンテンツを、あらかじめ定められた順序でのみ利用させる仕組みが実現できる。
【００８９】また、本実施例の変形として、２つのアクセスチケットを１回ずつ利用する事で、はじめて他のチケットを使用可能にするような仕組みも実現可能である。そのために、センタは以下のようなチケットと利用制限情報を用意する。
【００９０】アクセスチケットは次のようなものである。
【００９１】
【数７】ｔ１＝Ｄ１＋Ｆ（ｄｕ，Ｌ１，ｎ１）
ｔ２＝Ｄ２＋Ｆ（ｄｕ，Ｌ２，ｎ２）
ｔ３＝Ｄ３＋Ｆ（ｄｕ，Ｌ３，ｎ３）
利用制限情報は図１９に示すようなものである。
【００９２】上記の式および図１９において、Ｉｒ１、Ｉｒ２はチケット発行時に生成される乱数、Ｎはこのチケットを活性化させるのに必要な活性化情報の数である。また、ｆは使用履歴を示すフラグで、１度使われるとこの値は１に書き換えられる。
【００９３】ユーザにはｔ１からｔ３の一連のチケットと、利用制限情報Ｌ１～Ｌ３を含むアクセスチケットが配布される。但し、ユーザへの配布時には図２０に示すように、Ｌ３は、α３の値を０としたものに置き換えられる。
【００９４】ｔ１、ｔ２を最初に使用すると、それぞれの使用履歴が１に書き換えられるとともに、ｔ３のための活性化情報
【００９５】
【数８】α１′＝α１$^{F(du,L1,n1)}$
α２′＝α２$^{F(du,L2,n2)}$
が計算されて、Ｌ３に保持される。ｔ３を使用する際に、Ｎ３個の必要な活性化情報がそろっていた場合には、
【００９６】
【数９】α３＝α１′＋α２′＝α１$^{F(du,L1,n1)}$＋α２$^{F(du,L2,n2)}$
が計算できるので、ｔ３の使用が可能になる。
【００９７】このようにすることで、ｔ１、ｔ２の利用の順番を特定せずに、両方のチケットを使ったときのみ、ｔ３が有効になる仕組みを実現できる。
【００９８】
【発明の効果】以上のように、本発明を用いる事で、オフライン環境下においても、ユーザ環境および提供するコンテンツそのものに特段の機構を追加することなく、また、センタとのコンテンツの利用毎の通信を伴うこともなしに、暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御が可能になる。
【図面の簡単な説明】
【図１】　本発明の実施例１の構成を示すブロック図である。
【図２】　実施例１の処理を説明するフローチャートである。
【図３】　実施例１の処理を説明するフローチャートである。
【図４】　実施例１の鍵保持部の構造（初期値）を示す図である。
【図５】　実施例１の鍵保持部の構造（２番目の鍵Ｋ２が使用可能になった状態）を示す図である。
【図６】　本発明の実施例２で用いるアクセスチケットによる処理を説明する図である。
【図７】　アクセスチケットの構成を示す図である。

【図８】　実施例２の利用制限情報を説明する図である。
【図９】　実施例２の利用制限情報（ユーザに当初送られるもの）を説明する図である
【図１０】　実施例２のユーザ環境の構成を示すブロック図である。
【図１１】　実施例２の動作を説明するためのフローチャートである。
【図１２】　実施例２の動作を説明するためのフローチャートである。
【図１３】　実施例２の利用制限情報（最初のチケットを１回利用した後のもの）を説明する図である。
【図１４】　本発明の実施例３の利用制限情報を説明する図である。
【図１５】　実施例３の利用制限情報（ユーザに当初送られるもの）を説明する図である。
【図１６】　実施例３の動作を説明するフローチャートである。
【図１７】　実施例３の動作を説明するフローチャートである。
【図１８】　実施例３の利用制限情報（最初のチケットを１回利用した後のもの）を説明する図である。
【図１９】　実施例３の変形例の利用制限情報を説明する図である。
【図２０】　上述変形例の利用制限情報（ユーザに当初送られるもの）を説明する図である。
【符号の説明】
１０　利用環境（ホスト）
１１　暗号化コンテンツ保持部
１２　鍵保持部
２０　トークン
２１　鍵活性化情報演算部
２２　慣用暗号復号部２２

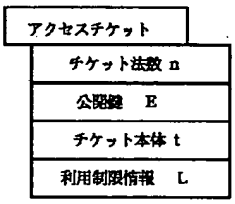
【図４】

鍵 ID	鍵	次の鍵 ID	鍵活性化情報	使用可能になるまでの回数
I_1	K_1	I_2	0	0
I_2	K_2'	I_3	0	Ur2
I_3	K_3'	I_4	0	Ur3
I_4	K_4'	0	0	Ur4

【図５】

鍵 ID	鍵	次の鍵 ID	鍵活性化情報	使用可能になるまでの回数
I_1	K_1	I_2	$\alpha_1'=F^{Ur1-1}(\alpha_1)$	0
I_2	$K_2=K_2'+F(\alpha_1')$	I_3	0	0
I_3	K_3'	I_4	0	Ur3
I_4	K_4'	0	0	Ur4

【図７】



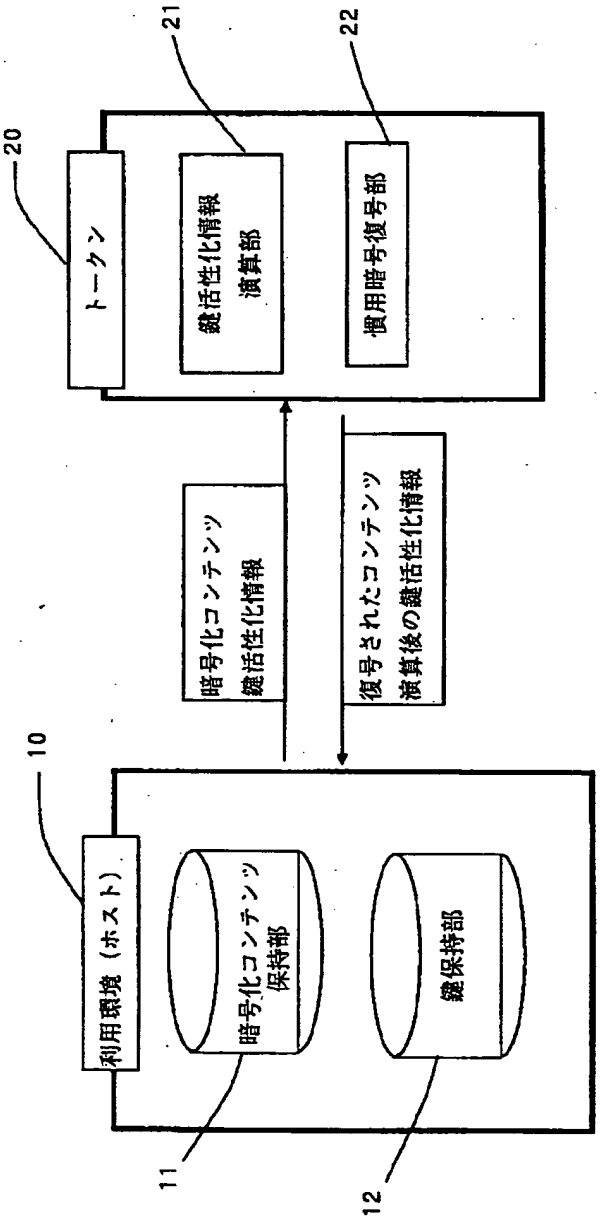
【図９】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	1	$Ur1=0$	$\alpha_1=Ir$
L_2	1997/12/31	80	2	$Ur2=20$	$\alpha_2=0$
L_3	1997/12/31	60	3	$Ur3=20$	$\alpha_3=0$
L_4	1997/12/31	40	4	$Ur4=20$	$\alpha_4=0$

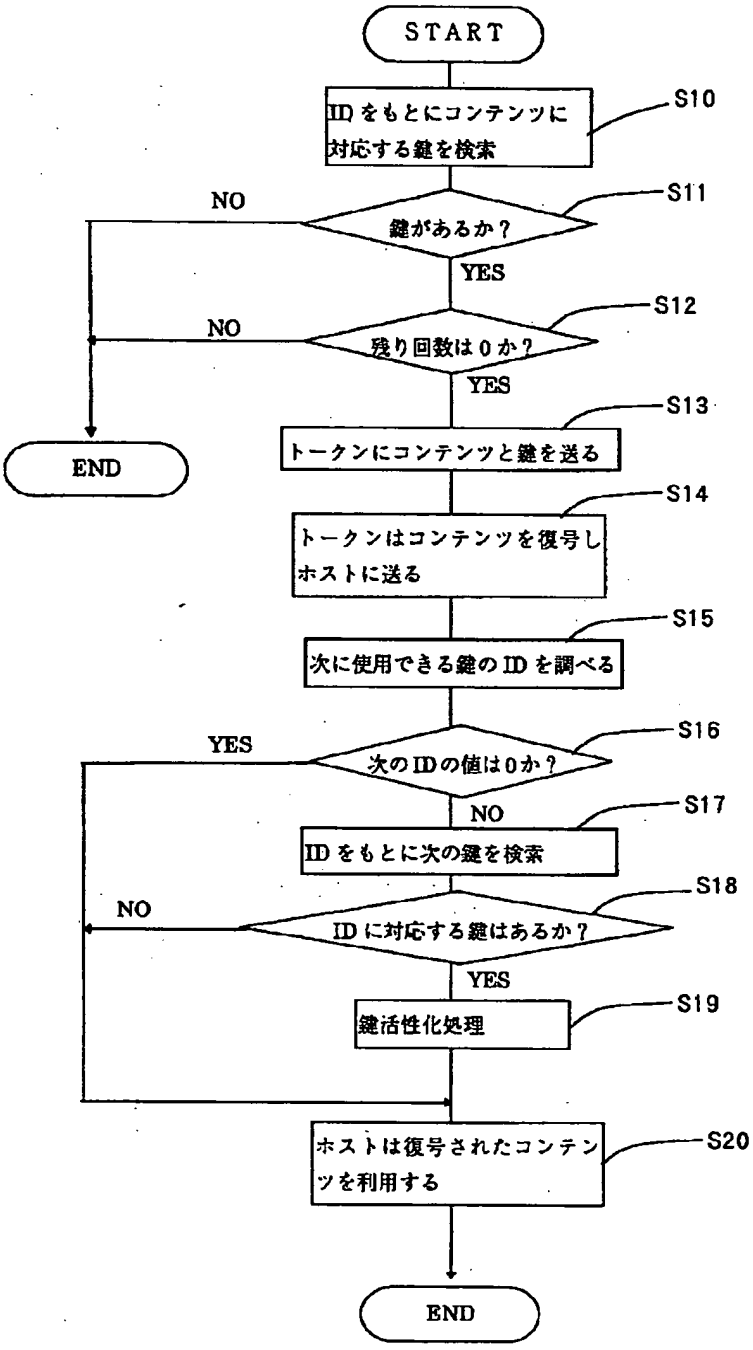
【図１３】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	1	$Ur1=0$	$\alpha_1=Ir$
L_2	1997/12/31	80	2	$Ur2=19$	$\alpha_2=(\alpha_1)^{Pub.L_2} \bmod n$
L_3	1997/12/31	60	3	$Ur3=20$	$\alpha_3=0$
L_4	1997/12/31	40	4	$Ur4=20$	$\alpha_4=0$

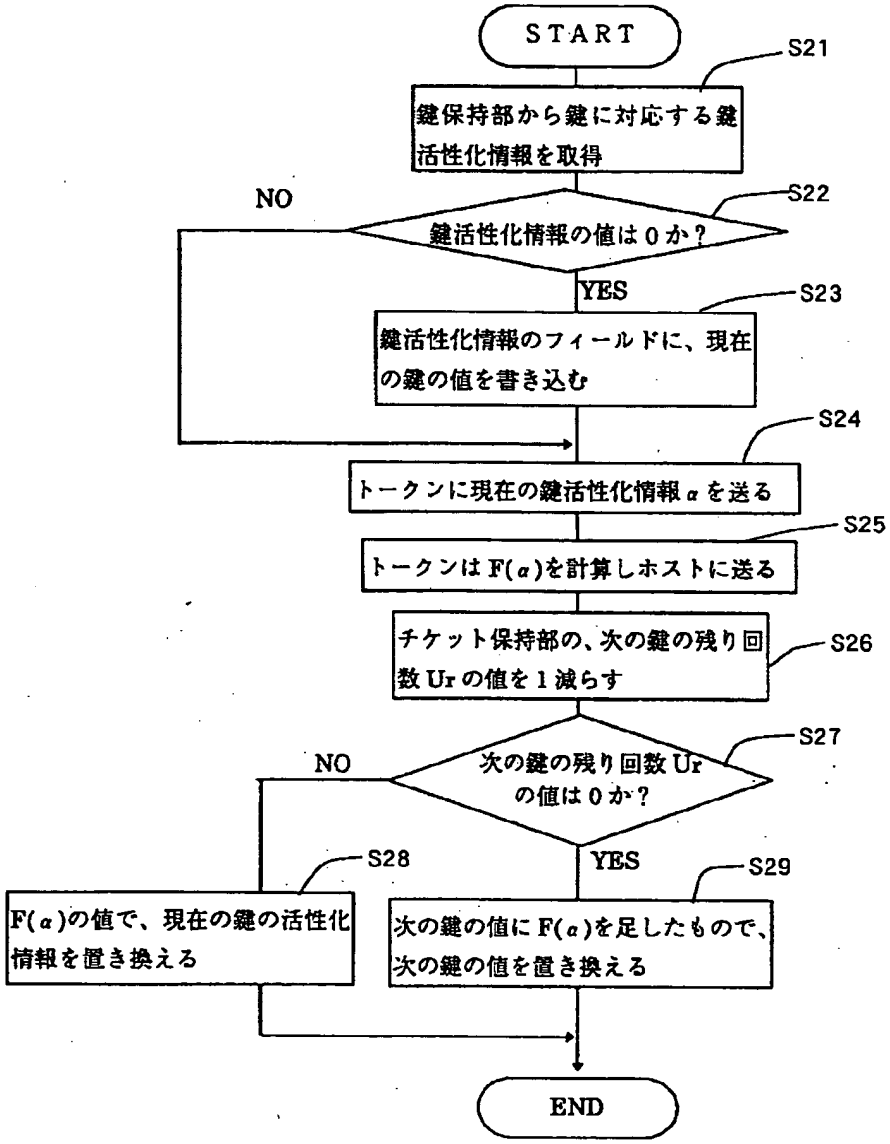
【図１】


20
トークン
21
鍵活性化情報
演算部
22
慣用暗号復号部
暗号化コンテンツ
鍵活性化情報
復号されたコンテンツ
演算後の鍵活性化情報
10
利用環境（ホスト）
暗号化コンテンツ
保持部
鍵保持部
11
12

【図２】


START
IDをもとにコンテンツに対応する鍵を検索
S10
鍵があるか？
S11
NO
YES
残り回数は０か？
S12
NO
YES
END
トークンにコンテンツと鍵を送る
S13
トークンはコンテンツを復号しホストに送る
S14
次に使用できる鍵のIDを調べる
S15
次のIDの値は0か？
S16
YES
NO
IDをもとに次の鍵を検索
S17
IDに対応する鍵はあるか？
S18
NO
YES
鍵活性化処理
S19
ホストは復号されたコンテンツを利用する
S20
END

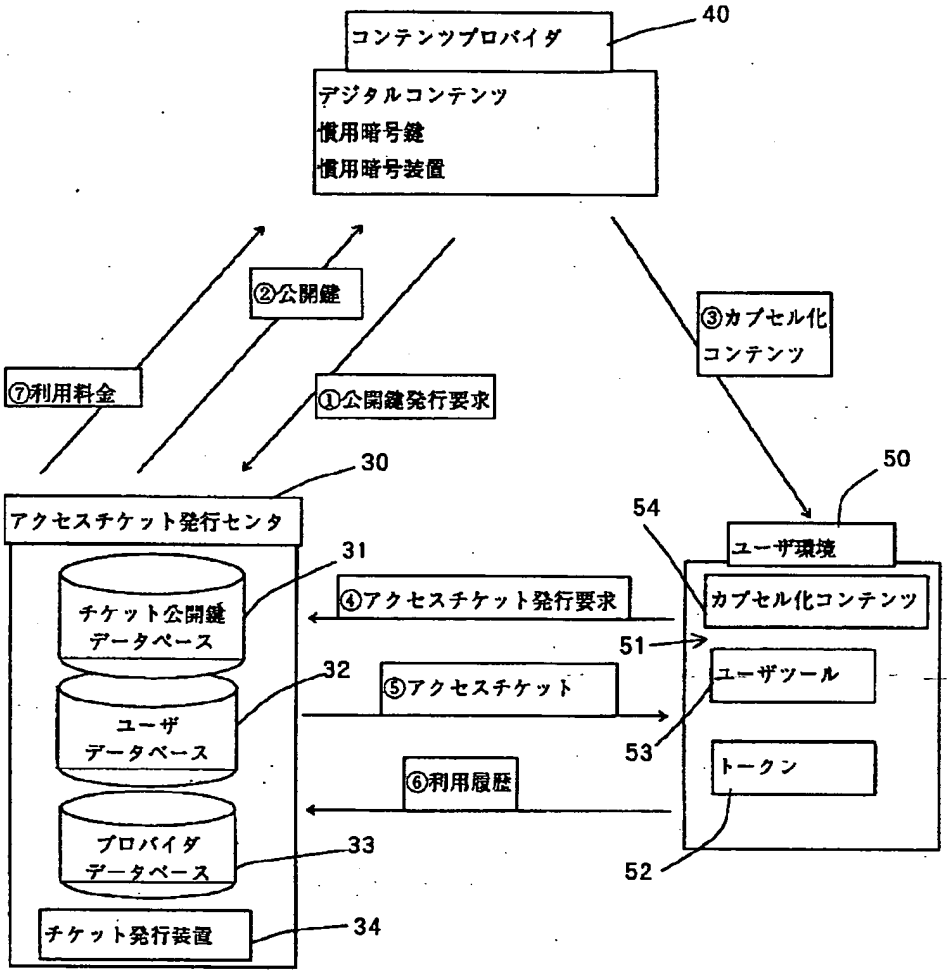
【図３】



【図１９】

利用制限情報	使用期限	利用料金	次のチケットの性数	使用履歴を示すフラグf	必要な活性化情報の数	チケット活性化情報α
L_1	1997/12/31	100	m_2	0	$N_1=1$	$\alpha_1=I_{n1}$
L_2	1997/12/31	100	m_3	0	$N_2=1$	$\alpha_2=I_{n2}$
L_3	1997/12/31	100	0	0	$N_3=2$	$\alpha_3=\alpha_2^{F(a_2,I_{n3})}+\alpha_1^{F(a_1,I_{n3})}$

【図６】



【図１４】

利用制限情報	使用期限	利用料金	次のチケットの件数	使用可能になるまでの回数 U_T	チケット活性化情報 α
L_1	1997/12/31	100	n_2	$U_T1=0$	$\alpha_1=I_T$
L_2	1997/12/31	100	n_3	$U_T2=0$	$\alpha_2=(\alpha_1)^{g(I_T,L_2,n_2)} \bmod n$: $U_T2=20$
L_3	1997/12/31	100	n_4	$U_T3=0$	$\alpha_3=(\alpha_2)^{g(I_T,L_3,n_3)} \bmod n$: $U_T3=20$
L_4	1997/12/31	100	0	$U_T4=0$	$\alpha_4=(\alpha_3)^{g(I_T,L_4,n_4)} \bmod n$: $U_T4=20$

【図８】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数 Ur	チケット活性化情報 α
L_1	1997/12/31	100	1	Ur1=0	$\alpha_1=Ir$
L_2	1997/12/31	80	2	Ur2=0	$\alpha_2=(\alpha_1)^{FUr2(du,L1,n)} \bmod n$: Ur2=20
L_3	1997/12/31	60	3	Ur3=0	$\alpha_3=(\alpha_2)^{FUr3(du,L2,n)} \bmod n$: Ur3=20
L_4	1997/12/31	40	4	Ur4=0	$\alpha_4=(\alpha_3)^{FUr4(du,L3,n)} \bmod n$: Ur4=20

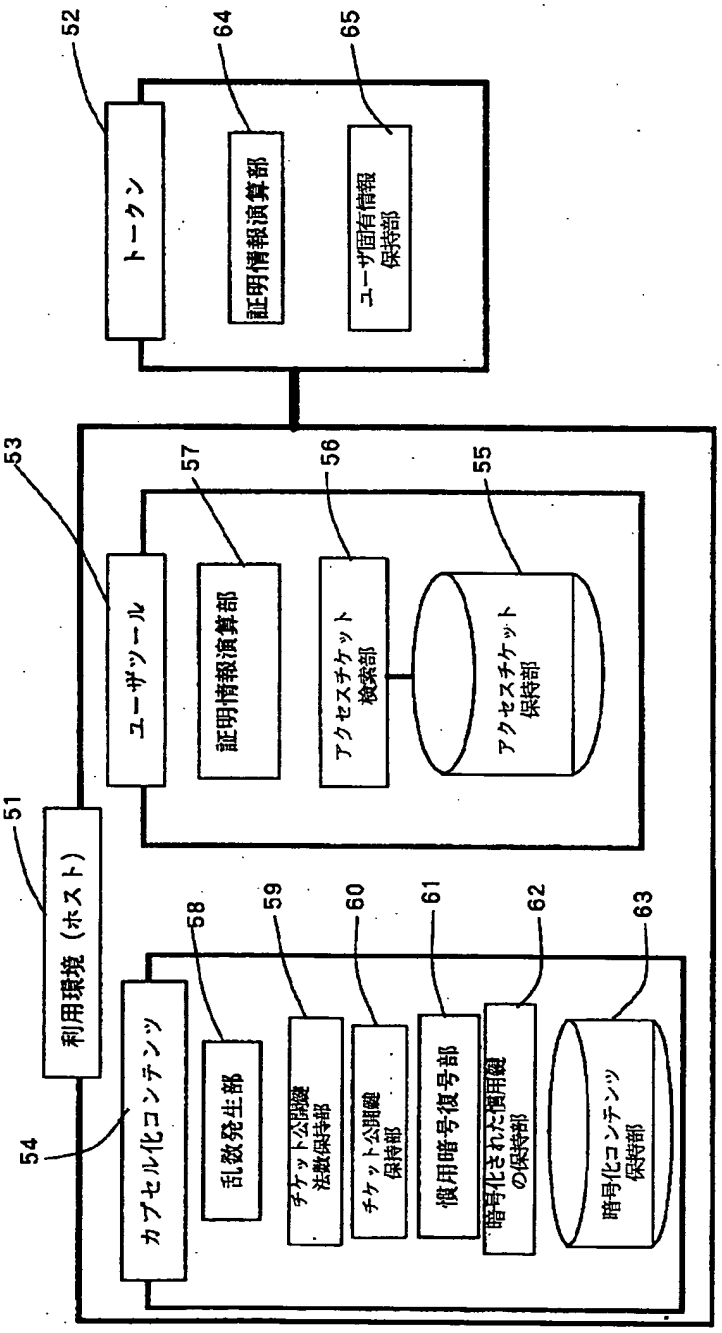
【図１５】

利用制限情報	使用期限	利用料金	次のチケットの法数	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	n_2	Ur1=0	$\alpha_1=Ir$
L_2	1997/12/31	100	n_3	Ur2=20	$\alpha_2=0$
L_3	1997/12/31	100	n_4	Ur3=20	$\alpha_3=0$
L_4	1997/12/31	100	0	Ur4=20	$\alpha_4=0$

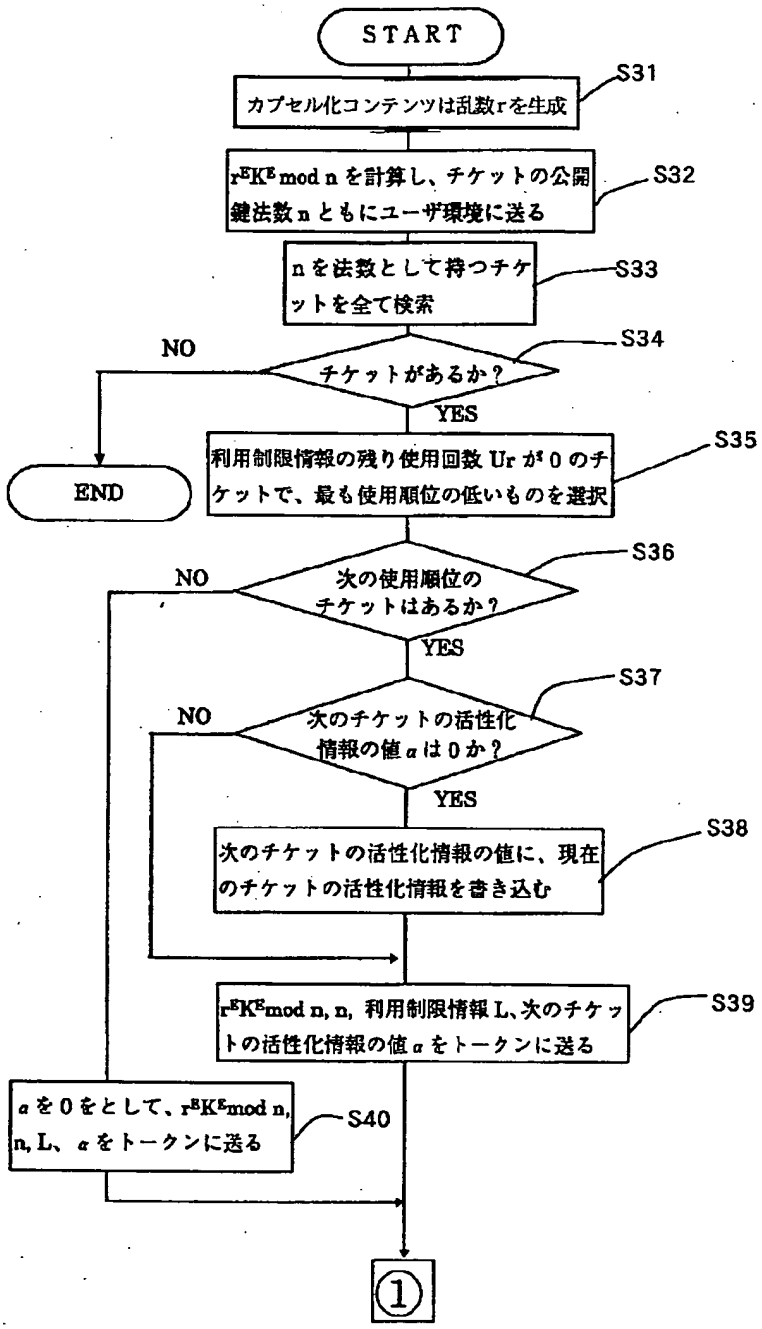
【図２０】

利用制限情報	使用期限	利用料金	次のチケットの法数	使用履歴を示すフラグf	必要な活性化情報の数	チケット活性化情報α
L_1	1997/12/31	100	n_2	0	$N_1=1$	$\alpha_1=Ir_1$
L_2	1997/12/31	100	n_3	0	$N_2=1$	$\alpha_2=Ir_2$
L_3	1997/12/31	100	0	0	$N_3=2$	$\alpha_3=0$

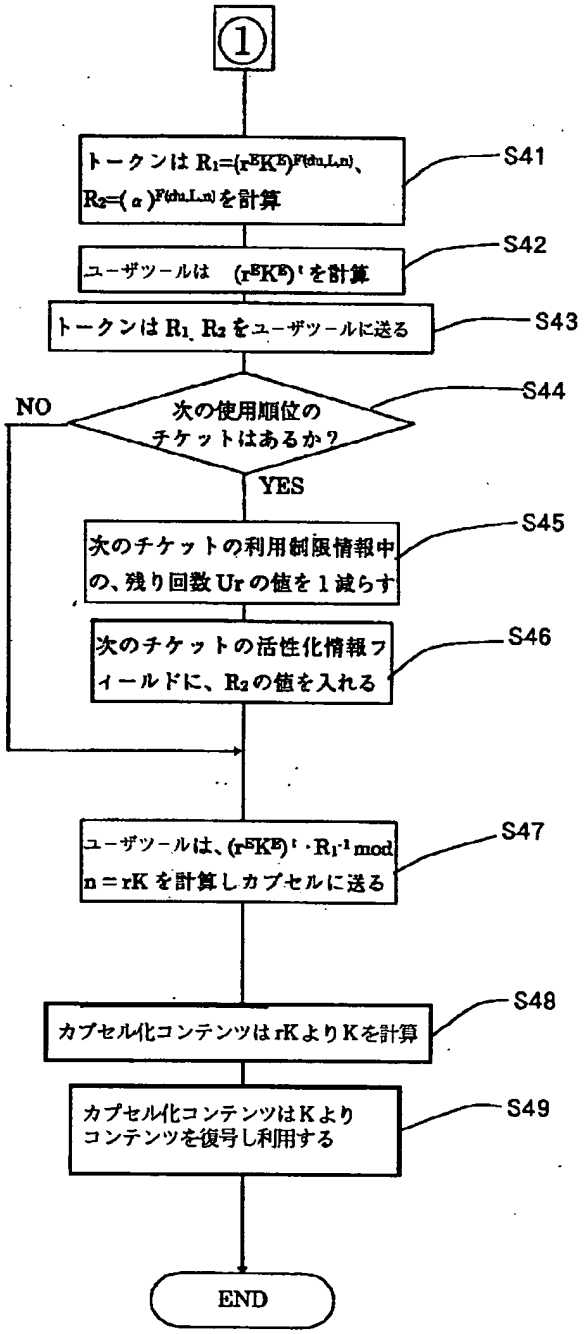
【図１０】


52
64
65
トークン
証明情報演算部
ユーザ固有情報保持部
53
57
56
55
ユーザツール
証明情報演算部
アクセスチケット検索部
アクセスチケット保持部
51
利用環境（ホスト）
58
59
60
61
62
63
カプセル化コンテンツ
乱数発生部
チケット公開鍵法数保持部
チケット公開鍵保持部
復用暗号復号部
暗号化された復用鍵の保持部
暗号化コンテンツ保持部
54

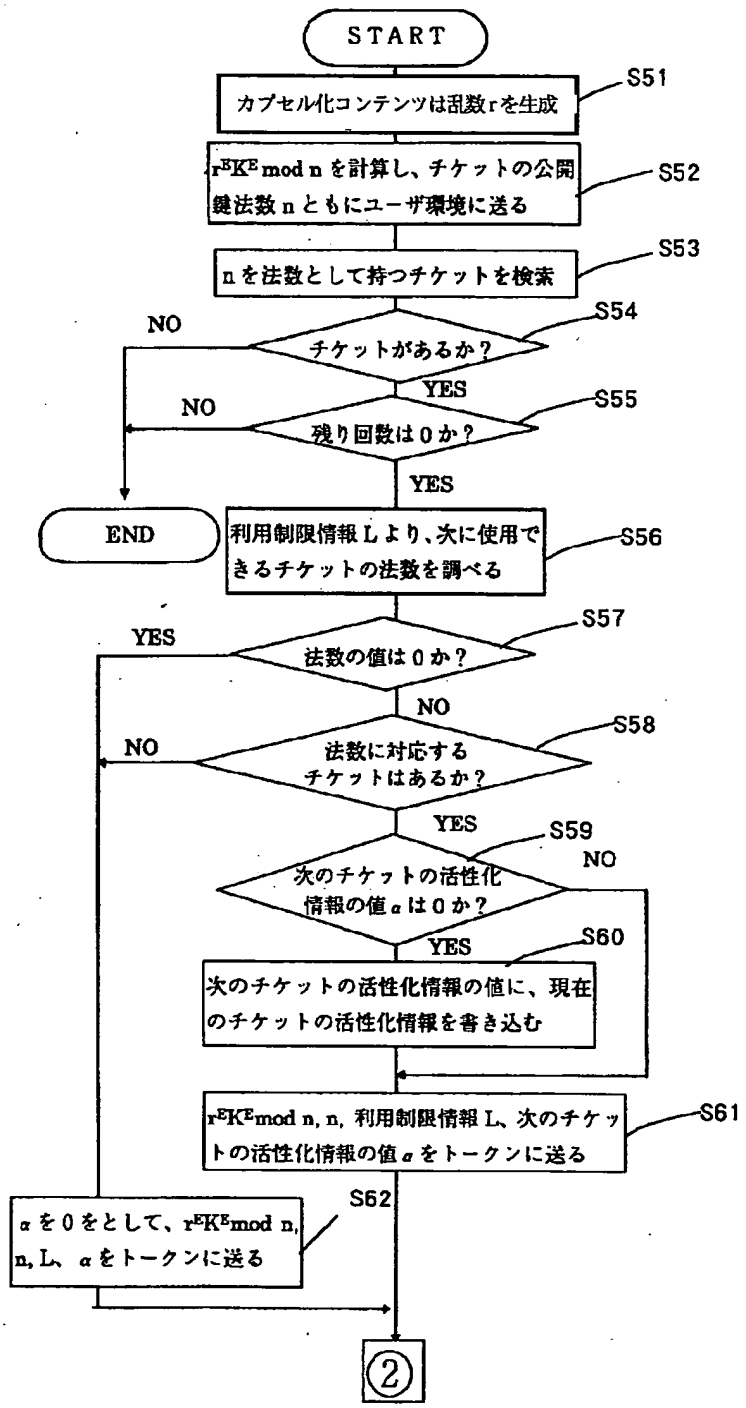
【図１１】


START
S31
カプセル化コンテンツは乱数rを生成
S32
$r^E K^E \bmod n$ を計算し、チケットの公開鍵法数nともにユーザ環境に送る
S33
nを法数として持つチケットを全て検索
S34
チケットがあるか？
NO
YES
END
S35
利用制限情報の残り使用回数 Ur が０のチケットで、最も使用順位の低いものを選択
S36
次の使用順位のチケットはあるか？
NO
YES
S37
次のチケットの活性化情報の値αは０か？
NO
YES
S38
次のチケットの活性化情報の値に、現在のチケットの活性化情報を書き込む
S39
$r^E K^E \bmod n$, n, 利用制限情報 L、次のチケットの活性化情報の値αをトークンに送る
S40
αを０をとして、$r^E K^E \bmod n$, n, L、αをトークンに送る
①

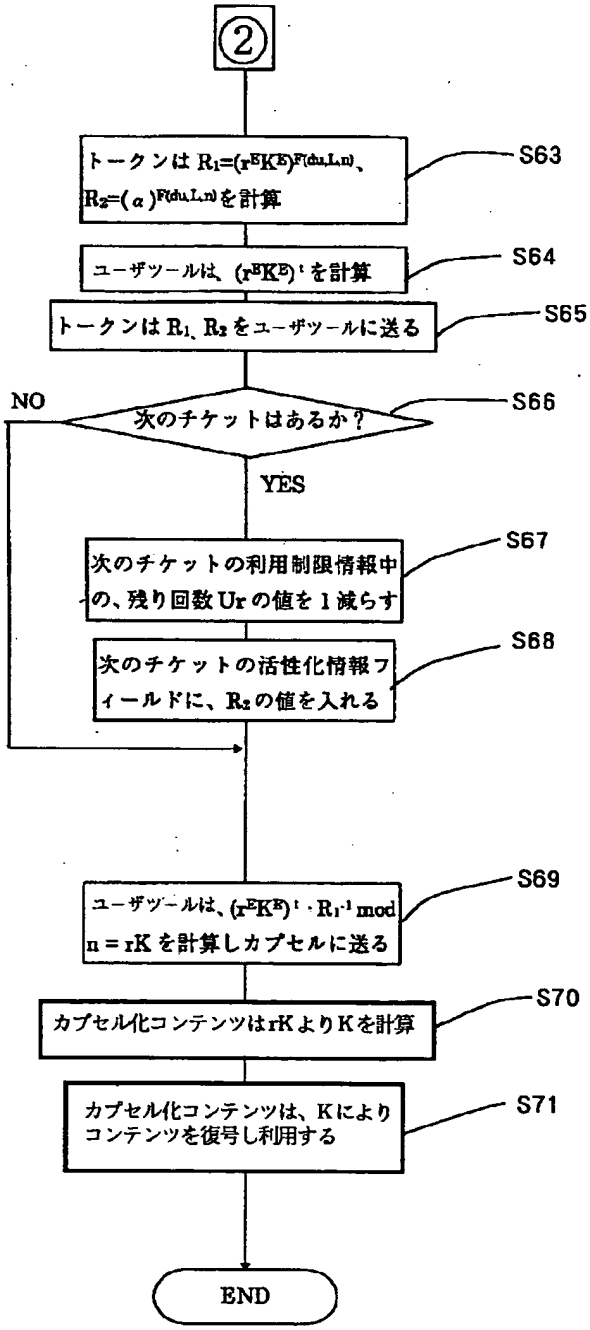
【図１２】


①
トークンは $R_1=(r^EK^E)^{F(du,L,n)}$、$R_2=(\alpha)^{F(du,L,n)}$を計算
S41
ユーザツールは $(r^EK^E)^t$を計算
S42
トークンは R_1、R_2をユーザツールに送る
S43
次の使用順位のチケットはあるか？
S44
NO
YES
次のチケットの利用制限情報中の、残り回数Urの値を１減らす
S45
次のチケットの活性化情報フィールドに、R_2の値を入れる
S46
ユーザツールは、$(r^EK^E)^t \cdot R_1^{-1} \bmod n = rK$を計算しカプセルに送る
S47
カプセル化コンテンツはrKよりKを計算
S48
カプセル化コンテンツはKよりコンテンツを復号し利用する
S49
END

【図１６】


START
S51
カプセル化コンテンツは乱数rを生成
$r^E K^E \bmod n$ を計算し、チケットの公開鍵法数nともにユーザ環境に送る
S52
nを法数として持つチケットを検索
S53
チケットがあるか？
S54
NO
YES
残り回数は0か？
S55
NO
YES
END
利用制限情報Lより、次に使用できるチケットの法数を調べる
S56
法数の値は0か？
S57
YES
NO
法数に対応するチケットはあるか？
S58
NO
YES
次のチケットの活性化情報の値αは0か？
S59
NO
YES
次のチケットの活性化情報の値に、現在のチケットの活性化情報を書き込む
S60
$r^E K^E \bmod n$, n, 利用制限情報L、次のチケットの活性化情報の値αをトークンに送る
S61
αを0をとして、$r^E K^E \bmod n$, n, L、αをトークンに送る
S62
②

【図１７】


②
トークンは $R_1=(r^E K^E)^{F(du,L,n)}$、$R_2=(\alpha)^{F(du,L,n)}$を計算
S63
ユーザツールは、$(r^E K^E)^{-1}$を計算
S64
トークンは R_1、R_2をユーザツールに送る
S65
NO
次のチケットはあるか？
S66
YES
次のチケットの利用制限情報中の、残り回数Urの値を１減らす
S67
次のチケットの活性化情報フィールドに、R_2の値を入れる
S68
ユーザツールは、$(r^E K^E)^{-1} \cdot R_1^{-1} \bmod n = rK$を計算しカプセルに送る
S69
カプセル化コンテンツはrKよりKを計算
S70
カプセル化コンテンツは、Kによりコンテンツを復号し利用する
S71
END

【図１８】

利用制限情報	使用期限	利用料金	次のチケットの法数	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	m_2	$U_{r1}=0$	$\sigma_1=I_r$
L_2	1997/12/31	100	m_3	$U_{r2}=19$	$\sigma_2=(\sigma_1)^{P_{pw,L_2,m_2}} \bmod n$
L_3	1997/12/31	100	m_4	$U_{r3}=20$	$\sigma_3=0$
L_4	1997/12/31	100	0	$U_{r4}=20$	$\sigma_4=0$

フロントページの続き

(51) Int. Cl.⁶	識別記号	F I	
// G06F 12/14	320	H04L 9/00	601E
			641

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-244584

(43)Date of publication of application : 19.09.1995

(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 06-032601

(22)Date of filing : 02.03.1994

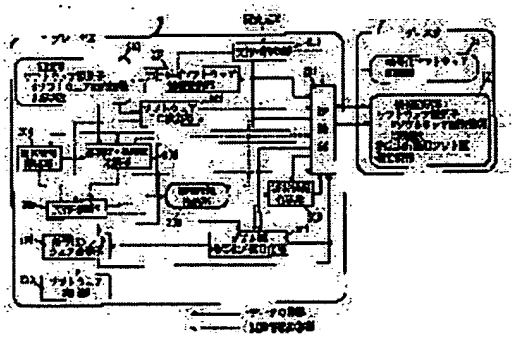
(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(72)Inventor : OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO
MIYAJI MITSUKO

(54) SOFTWARE PROTECTION SYSTEM

(57)Abstract:

PURPOSE: To attain execution by an optional execution device by a procedure for changing a specified execution device in a software protection system which can not be executed by an execution device other than the specified one.



CONSTITUTION: Whether a software identifier(ID) recorded in an information recording part 12 of a disk 1 is stored in a storage part 203 or not is retrieved. When the corresponding ID is stored in the storage part 203, the accumulated number of IDs is compared with a reference number stored in the storage part 203, and only when the accumulated number is larger, the execution of the software is permitted. Also when the corresponding ID is not stored in the storage part 203, the execution of the software is permitted. In this case, a software key in the recording part 12 is decoded by a software key ciphering/ decoding part 207, ciphered software recorded in a ciphered software recording part 11 is decoded by using the software key and executed by a software execution part 210. At the time of changing a specified execution device, the accumulated number of IDs and the reference value are changed and a software key is

rewritten to a key for a changed execution device.